NETGEAR

ProSafe Wireless-N 8-Port Gigabit VPN Firewall FVS318N

Reference Manual

350 East Plumeria Drive
San Jose, CA 95134
USA

September 2011
202-10836-01
1.0

© 2011 NETGEAR, Inc. All rights reserved.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of NETGEAR, Inc.

Technical Support

Thank you for choosing NETGEAR. To register your product, get the latest product updates, get support online, or for more information about the topics covered in this manual, visit the Support website at *http://support.netgear.com.*

Phone (US & Canada only): 1-888-NETGEAR

Phone (Other Countries): Check the list of phone numbers at *http://support.netgear.com/app/answers/detail/a_id/984*.

Trademarks

NETGEAR, the NETGEAR logo, and Connect with Innovation are trademarks and/or registered trademarks of NETGEAR, Inc. and/or its subsidiaries in the United States and/or other countries. Information is subject to change without notice. Other brand and product names are registered trademarks or trademarks of their respective holders. © 2011 NETGEAR, Inc. All rights reserved.

Statement of Conditions

To improve internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice. NETGEAR does not assume any liability that may occur due to the use, or application of, the product(s) or circuit layout(s) described herein.

Revision History

Publication Part Number	Version	Publish Date	Comments
202-10836-01	1.0	September 2011	First publication

Contents

Chapter 1 Introduction

What Is the ProSafe Wireless-N 8-Port Gigabit VPN Firewall FVS318N? . . 9
Key Features and Capabilities 10
Wireless Features. 10
Advanced VPN Support for Both IPSec and SSL. 11
A Powerful, True Firewall 11
Security Features 12
Autosensing Ethernet Connections with Auto Uplink 12
Extensive Protocol Support 12
Easy Installation and Management 13
Maintenance and Support 14
Package Contents 14
Hardware Features. 14
Front Panel 14
Rear Panel 17
Bottom Panel with Product Label 18
Choose a Location for the Wireless VPN Firewall 18

Chapter 2 Internet and Broadband Settings

Log In to the Wireless VPN Firewall 19
Web Management Interface Menu Layout 21
Requirements for Entering IP Addresses 23
Internet and WAN Configuration Tasks 23
Set Up an IPv4 Internet Connection to Your ISP 24
Set Up an IPv6 Internet Connection to Your ISP 24
Configure the IPv4 Internet Connection 24
Let the Wireless VPN Firewall Automatically Detect and Configure an IPv4 Internet Connection 25
Manually Configure an IPv4 Internet Connection 27
Configure the IPv4 WAN Mode 31
Configure the IPv6 Internet Connection 32
Let the Wireless VPN Firewall Automatically Configure an IPv6 Internet Connection 33
Manually Configure an IPv6 Internet Connection 34
Configure IPv6 Settings 36
Configure the IPv6 Routing Mode 36
Configure IPv6 Tunnels 37
Configure Dynamic DNS 40
Configure Advanced WAN Options and Other Tasks. 43

Additional WAN-Related Configuration Tasks 45
Verify the Connection 45
What to Do Next 45

Chapter 3 LAN Configuration

Manage IPv4 Virtual LANs and DHCP Options 46
Port-Based VLANs 47
Assign and Manage VLAN Profiles 48
VLAN DHCP Options 49
Configure a VLAN Profile 51
Configure VLAN MAC Addresses and LAN Advanced Settings. 56
Configure IPv4 Multihome LAN IP Addresses on the Default VLAN 57
Manage IPv4 Groups and Hosts (IPv4 LAN Groups). 59
Manage the Network Database 60
Change Group Names in the Network Database 63
Set Up Address Reservation 64
Configure IPv6 LAN Settings 64
Configure the Router Advertisement Daemon and Advertisement Prefixes. 68
Configure and Enable the DMZ Port for IPv4 Traffic 72
Manage Static IPv4 Routing. 76
Configure Static IPv4 Routes 76
Configure the Routing Information Protocol 78
IPv4 Static Route Example. 81
Manage Static IPv6 Routing. 81

Chapter 4 Wireless Configuration and Security

Overview of the Wireless Features 84
Wireless Equipment Placement and Range Guidelines. 85
Configure the Basic Radio Settings 86
Operating Frequency (Channel) Guidelines. 88
Wireless Data Security Options 89
Wireless Security Profiles. 91
Before You Change the SSID, WEP, and WPA Settings 92
Configure and Enable Wireless Security Profiles. 93
Configure Virtual Access Points. 98
Restrict Wireless Access by MAC Address 101
Configure Wi-Fi Protected Setup 102
Configure Advanced Radio Settings 104
Test Basic Wireless Connectivity 105

Chapter 5 IPv4 Firewall Protection

About IPv4 Firewall Protection 107
Administrator Tips. 108
Rules to Block or Allow Specific Kinds of Traffic 108
Service-Based Rules 109

Order of Precedence for Rules 115
Set LAN WAN Rules 116
Create DMZ WAN Rules 119
Create LAN DMZ Rules 122
Inbound Rule Examples 126
Outbound Rule Example 131
Configure Other Firewall Features 132
Attack Checks 132
Set Session Limits 134
Manage the Application Level Gateway for SIP Sessions 135
Services, Bandwidth Profiles, and QoS Profiles 136
Add Customized Services 136
Create Bandwidth Profiles 139
Preconfigured Quality of Service Profiles 141
Configure Content Filtering 142
Set a Schedule to Block or Allow Specific Traffic 146
Enable Source MAC Filtering 147
Set Up IP/MAC Bindings 148
Configure Port Triggering 151
Configure Universal Plug and Play 153

Chapter 6 Virtual Private Networking Using IPv4 IPSec and L2TP Connections

Use the IPSec VPN Wizard for Client and Gateway Configurations 156
Create a Gateway-to-Gateway VPN Tunnel with the Wizard 156
Create a Client-to-Gateway VPN Tunnel 160
Test the Connection and View Connection and Status Information 175
Test the NETGEAR VPN Client Connection 175
NETGEAR VPN Client Status and Log Information 176
View the Wireless VPN Firewall IPSec VPN Connection Status 177
View the Wireless VPN Firewall IPSec VPN Log 178
Manage IPSec VPN Policies 179
Manage IKE Policies 179
Manage VPN Policies 187
Configure Extended Authentication (XAUTH) 194
Configure XAUTH for VPN Clients 195
User Database Configuration 196
RADIUS Client Configuration 196
Assign IP Addresses to Remote Users (Mode Config) 198
Mode Config Operation 199
Configure Mode Config Operation on the Wireless VPN Firewall 199
Configure the ProSafe VPN Client for Mode Config Operation 206
Test the Mode Config Connection 213
Modify or Delete a Mode Config Record 214
Configure Keep-Alives and Dead Peer Detection 215
Configure Keep-Alives 215
Configure Dead Peer Detection 216

Configure NetBIOS Bridging with IPSec VPN 217
Configure the L2TP Server. 218
View the Active L2TP Users 219

Chapter 7 Virtual Private Networking Using IPv4 SSL Connections

SSL VPN Portal Options 222
Overview of the SSL Configuration Process 222
Create the Portal Layout. 223
Configure Domains, Groups, and Users 227
Configure Applications for Port Forwarding 227
Add Servers and Port Numbers 227
Add a New Host Name 229
Configure the SSL VPN Client 230
Add Routes for VPN Tunnel Clients 232
Use Network Resource Objects to Simplify Policies 233
Add New Network Resources. 233
Edit Network Resources to Specify Addresses 234
Configure User, Group, and Global Policies 235
View Policies 237
Add a Policy 237
Access the New SSL Portal Login Screen 241
View the SSL VPN Connection Status 243
View the SSL VPN Log. 244

Chapter 8 Manage Users, Authentication, and VPN Certificates

The Wireless VPN Firewall's Authentication Process and Options 245
Configure Authentication Domains, Groups, and Users. 247
Configure Domains. 247
Configure Groups 251
Configure User Accounts 254
Set User Login Policies 257
Change Passwords and Other User Settings. 261
Manage Digital Certificates for VPN Connections 262
VPN Certificates Screen. 263
Manage VPN CA Certificates 264
Manage VPN Self-Signed Certificates 265
Manage the VPN Certificate Revocation List 269

Chapter 9 Network and System Management

Performance Management. 270
Bandwidth Capacity 270
Features That Reduce Traffic. 270
Features That Increase Traffic 273
Use QoS and Bandwidth Assignment to Shift the Traffic Mix. 275
Monitoring Tools for Traffic Management. 276

System Management 276
Change Passwords and Administrator and Guest Settings 276
Configure Remote Management Access 278
Use a Simple Network Management Protocol Manager 281
Manage the Configuration File 284
Configure Date and Time Service 288

Chapter 10 Monitor System Access and Performance

Enable the WAN Traffic Meter 290
Configure Logging, Alerts, and Event Notifications 293
How to Send Syslogs over a VPN Tunnel between Sites 297
View Status Screens 300
View the System Status 300
View the VPN Connection Status and L2TP Users 307
View the VPN Logs 309
View the Port Triggering Status 310
View the WAN Port Status 311
View the Attached Devices and the DHCP Log 313
Diagnostics Utilities 316
Send a Ping Packet 316
Trace a Route 317
Look Up a DNS Address 317
Display the Routing Tables 317
Capture Packets in Real Time 318
Reboot the Wireless VPN Firewall Remotely 318

Chapter 11 Troubleshooting

Basic Functioning 320
Power LED Not On 320
Test LED Never Turns Off 320
LAN or WAN Port LEDs Not On 321
Troubleshoot the Web Management Interface 321
When You Enter a URL or IP Address, a Time-Out Error Occurs 322
Troubleshoot the ISP Connection 323
Troubleshooting the IPv6 Connection 324
Troubleshoot a TCP/IP Network Using a Ping Utility 327
Test the LAN Path to Your Wireless VPN Firewall 327
Test the Path from Your PC to a Remote Device 328
Restore the Default Configuration and Password 328
Address Problems with Date and Time 330
Access the Knowledge Base and Documentation 330

Appendix A Default Settings and Technical Specifications

Default Settings 331
Physical and Technical Specifications 333

Appendix B Two-Factor Authentication

Why Do I Need Two-Factor Authentication? 336
What Are the Benefits of Two-Factor Authentication? 336
What Is Two-Factor Authentication? 337
NETGEAR Two-Factor Authentication Solutions 337

Appendix C Notification of Compliance (Wired)

Appendix D Notification of Compliance (Wireless)

Index

Introduction

1

This chapter provides an overview of the features and capabilities of the ProSafe Wireless-N 8-Port Gigabit VPN Firewall FVS318N. This chapter contains the following sections:

- *What Is the ProSafe Wireless-N 8-Port Gigabit VPN Firewall FVS318N?*
- *Key Features and Capabilities*
- *Package Contents*
- *Hardware Features*
- *Choose a Location for the Wireless VPN Firewall*

Note: For more information about the topics covered in this manual, visit the NETGEAR support website at *http://support.netgear.com*.

What Is the ProSafe Wireless-N 8-Port Gigabit VPN Firewall FVS318N?

The ProSafe Wireless-N 8-Port Gigabit VPN Firewall FVS318N, hereafter referred to as the wireless VPN firewall, connects your local area network (LAN) and wireless LAN (WLAN) to the Internet through an external broadband access device such as a modem or radio antenna, or another router. A 2.4-GHz radio supports wireless connections in 802.11n mode with support for legacy clients in 802.11b and 802.11g mode.

The wireless VPN firewall routes both IPv4 and IPv6 traffic. A powerful, flexible firewall protects your IPv4 network from denial of service (DoS) attacks, unwanted traffic, and traffic with objectionable content. IPv6 traffic is supported through 6to4 and Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) tunnels.

The wireless VPN firewall provides advanced IPSec and SSL VPN technologies as well as L2TP support for easy and secure remote connections. The use of Gigabit Ethernet WAN and LAN ports ensures high data transfer speeds.

Key Features and Capabilities

The wireless VPN firewall provides the following key features and capabilities:

- A single 10/100/1000 Mbps Gigabit Ethernet WAN port
- Built-in eight-port 10/100/1000 Mbps Gigabit Ethernet LAN switch for extremely fast data transfer between local network resources
- A wireless radio with up to four virtual access points (VAPs)
- Both IPv4 and IPv6 support
- Advanced IPSec VPN and SSL VPN support
- L2TP tunnel support
- Advanced Stateful Packet Inspection (SPI) firewall with multi-NAT support
- SNMP manageable
- Front panel LEDs for easy monitoring of status and activity
- Flash memory for firmware upgrade
- Internal universal switching power supply

Wireless Features

The wireless VPN firewall supports the following features:

- **2.4 GHz radio**. 2.4-GHz band support with 802.11b/g/n wireless modes.
- **Virtual access points**. Support for up to four virtual access points (VAPs), each with its own SSID and security profile.
- **Access control**. The Media Access Control (MAC) address filtering feature can ensure that only trusted wireless stations can use the wireless VPN firewall to gain access to your LAN.
- **Hidden mode**. The SSID is not broadcast, assuring that only clients configured with the correct SSID can connect.
- **Secure and economical operation**. Adjustable power output allows more secure or economical operation.

Advanced VPN Support for Both IPSec and SSL

The wireless VPN firewall supports IPSec and SSL virtual private network (VPN) connections:

- IPSec VPN delivers full network access between a central office and branch offices, or between a central office and telecommuters. Remote access by telecommuters requires the installation of VPN client software on the remote computer.
  - IPSec VPN with broad protocol support for secure connection to other IPSec gateways and clients.
  - Up to twelve simultaneous IPSec VPN connections.
  - Bundled with a 30-day trial license for the ProSafe VPN Client software (VPN01L).
- SSL VPN provides remote access for mobile users to selected corporate resources without requiring a preinstalled VPN client on their computers.
  - Uses the familiar Secure Sockets Layer (SSL) protocol, commonly used for e-commerce transactions, to provide client-free access with customizable user portals and support for a wide variety of user repositories.
  - Up to five simultaneous SSL VPN connections.
  - Allows browser-based, platform-independent remote access through a number of popular browsers, such as Microsoft Internet Explorer, Mozilla Firefox, and Apple Safari.
  - Provides granular access to corporate resources based on user type or group membership.

A Powerful, True Firewall

Unlike simple NAT routers, the wireless VPN firewall is a true firewall, using Stateful Packet Inspection (SPI) to defend against hacker attacks. Its firewall features have the following capabilities:

- **DoS protection**. Automatically detects and thwarts denial of service (DoS) attacks such as Ping of Death and SYN flood.
- **Secure firewall**. Blocks unwanted traffic from the Internet to your LAN.
- **Schedule policies**. Permits scheduling of firewall policies by day and time.
- **Logs security incidents**. Logs security events such as blocked incoming traffic, port scans, attacks, and administrator logins. You can configure the firewall to email the log to you at specified intervals. You can also configure the firewall to send immediate alert messages to your email address or email pager whenever a significant event occurs.

Security Features

The wireless VPN firewall is equipped with several features designed to maintain security:

- **PCs hidden by NAT**. NAT opens a temporary path to the Internet for requests originating from the local network. Requests originating from outside the LAN are discarded, preventing users outside the LAN from finding and directly accessing the computers on the LAN.
- **Port forwarding with NAT**. Although NAT prevents Internet locations from directly accessing the PCs on the LAN, the wireless VPN firewall allows you to direct incoming traffic to specific PCs based on the service port number of the incoming request.
- **DMZ port**. Incoming traffic from the Internet is usually discarded by the wireless VPN firewall unless the traffic is a response to one of your local computers or a service for which you have configured an inbound rule. Instead of discarding this traffic, you can use the dedicated demilitarized zone (DMZ) port to forward the traffic to one PC on your network.

Autosensing Ethernet Connections with Auto Uplink

With its internal eight-port 10/100/1000 Mbps switch and 10/100/1000 WAN port, the wireless VPN firewall can connect to either a 10 Mbps standard Ethernet network, a 100 Mbps Fast Ethernet network, or a 1000 Mbps Gigabit Ethernet network. The LAN and WAN interfaces are autosensing and capable of full-duplex or half-duplex operation.

The wireless VPN firewall incorporates Auto Uplink™ technology. Each Ethernet port automatically senses whether the Ethernet cable plugged into the port should have a *normal* connection such as to a PC or an *uplink* connection such as to a switch or hub. That port then configures itself correctly. This feature eliminates the need for you to think about crossover cables, as Auto Uplink accommodates either type of cable to make the right connection.

Extensive Protocol Support

The wireless VPN firewall supports the Transmission Control Protocol/Internet Protocol (TCP/IP) and Routing Information Protocol (RIP). The wireless VPN firewall provides the following protocol support:

- **IP address sharing by NAT**. The wireless VPN firewall allows many networked PCs to share an Internet account using only a single IP address, which might be statically or dynamically assigned by your Internet service provider (ISP). This technique, known as Network Address Translation (NAT), allows the use of an inexpensive single-user ISP account.
- **Automatic configuration of attached PCs by DHCP**. The wireless VPN firewall dynamically assigns network configuration information, including IP, gateway, and Domain Name Server (DNS) addresses, to attached PCs on the LAN using the Dynamic Host Configuration Protocol (DHCP). This feature greatly simplifies configuration of PCs on your local network.

- **DNS proxy**. When DHCP is enabled and no DNS addresses are specified, the firewall provides its own address as a DNS server to the attached PCs. The firewall obtains actual DNS addresses from the ISP during connection setup and forwards DNS requests from the LAN.
- **PPP over Ethernet (PPPoE)**. PPPoE is a protocol for connecting remote hosts to the Internet over a DSL connection by simulating a dial-up connection.
- **Quality of Service (QoS)**. The wireless VPN firewall supports QoS.
- **Layer 2 Tunneling Protocol (L2TP)**. A tunneling protocol that is used to support virtual private networks (VPNs).

Easy Installation and Management

You can install, configure, and operate the wireless VPN firewall within minutes after connecting it to the network. The following features simplify installation and management tasks:

- **Browser-based management**. Browser-based configuration allows you to easily configure the wireless VPN firewall from almost any type of operating system, such as Windows, Macintosh, or Linux. Online help documentation is built into the browser-based web management interface.
- **Auto-detection of ISP**. The wireless VPN firewall automatically senses the type of Internet connection, asking you only for the information required for your type of ISP account.
- **IPSec VPN Wizard**. The wireless VPN firewall includes the NETGEAR IPSec VPN Wizard so you can easily configure IPSec VPN tunnels according to the recommendations of the Virtual Private Network Consortium (VPNC). This ensures that the IPSec VPN tunnels are interoperable with other VPNC-compliant VPN routers and clients.
- **SNMP**. The wireless VPN firewall supports the Simple Network Management Protocol (SNMP) to let you monitor and manage log resources from an SNMP-compliant system manager. The SNMP system configuration lets you change the system variables for MIB2.
- **Diagnostic functions**. The wireless VPN firewall incorporates built-in diagnostic functions such as ping, traceroute, DNS lookup, and remote reboot.
- **Remote management**. The wireless VPN firewall allows you to log in to the web management interface from a remote location on the Internet. For security, you can limit remote management access to a specified remote IP address or range of addresses.
- **Visual monitoring**. The wireless VPN firewall's front panel LEDs provide an easy way to monitor its status and activity.

Maintenance and Support

NETGEAR offers the following features to help you maximize your use of the wireless VPN firewall:

- Flash memory for firmware upgrades.
- Technical support seven days a week, 24 hours a day. Information about support is available on the NETGEAR website at *http://support.netgear.com/app/answers/detail/a_id/212*.

Package Contents

The wireless VPN firewall product package contains the following items:

- ProSafe Wireless-N 8-Port Gigabit VPN Firewall FVS318N
- One 12V 1A power supply unit for your region
- Rubber feet
- *Resource CD*, including:
  - Application Notes and other helpful information
  - 30-day trial license for the ProSafe VPN Client software (VPN01L)

If any of the parts are incorrect, missing, or damaged, contact your NETGEAR dealer. Keep the carton, including the original packing materials, in case you need to return the product for repair.

Hardware Features

The front panel ports and LEDs, rear panel ports, and bottom label of the wireless VPN firewall are described in the following sections.

Front Panel

Viewed from left to right, the wireless VPN firewall front panel contains the following ports:

- LAN Ethernet ports. Eight switched N-way automatic speed negotiating, Auto MDI/MDIX, Gigabit Ethernet ports with RJ-45 connectors.
- WAN Ethernet port. One independent N-way automatic speed negotiating, Auto MDI/MDIX, Gigabit Ethernet port with an RJ-45 connector.

The front panel also contains three groups of status indicator light-emitting diodes (LEDs), including Power and Test LEDs, LAN LEDs, and WAN LEDs, all of which are explained in detail in the following table. Some LED explanation is provided on the front panel.

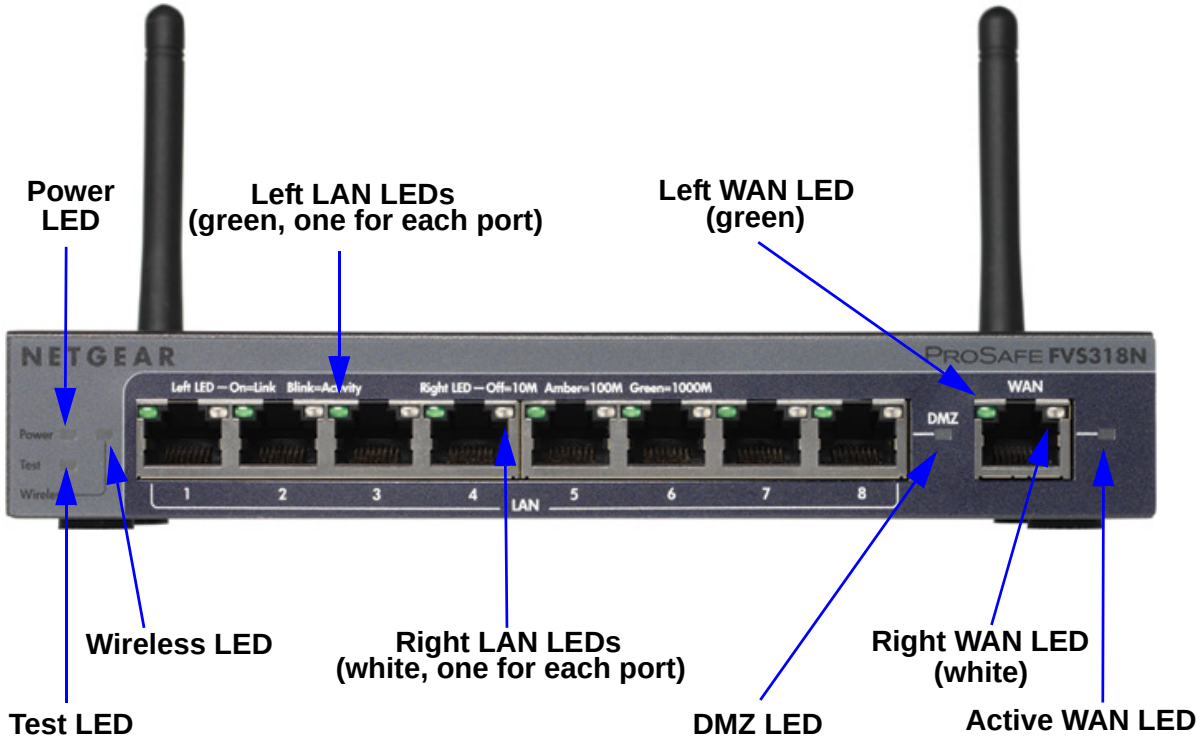


Figure 1.

The following table describes the function of each LED.

Table 1. LED descriptions

LED	Activity	Description
Power LED	On (green)	Power is supplied to the wireless VPN firewall.
	Off	Power is not supplied to the wireless VPN firewall.
Test LED	On (amber) during startup.	Test mode. The wireless VPN firewall is initializing. After approximately 2 minutes, when the wireless VPN firewall has completed its initialization, the Test LED goes off.
	On (amber) during any other time	The initialization has failed, or a hardware failure has occurred.
	Blinking (amber)	The wireless VPN firewall is writing to flash memory (during upgrading or resetting to defaults).
	Off	The wireless VPN firewall has booted successfully.

Table 1. LED descriptions (continued)

LED	Activity	Description
LAN Ports		
Left LED	Off	The LAN port has no link.
	On (green)	The LAN port has detected a link with a connected Ethernet device.
	Blinking (green)	Data is being transmitted or received by the LAN port.
Right LED	Off	The LAN port is operating at 10 Mbps.
	On (amber)	The LAN port is operating at 100 Mbps.
	On (green)	The LAN port is operating at 1000 Mbps.
DMZ LED	Off	Port 8 is operating as a normal LAN port.
	On (green)	Port 8 is operating as a dedicated hardware DMZ port.
WAN Port		
Left LED	Off	The WAN port has no physical link, that is, no Ethernet cable is plugged into the wireless VPN firewall.
	On (green)	The WAN port has a valid connection with a device that provides an Internet connection.
	Blinking (green)	Data is being transmitted or received by the WAN port.
Right LED	Off	The WAN port is operating at 10 Mbps.
	On (amber)	The WAN port is operating at 100 Mbps.
	On (green)	The WAN port is operating at 1000 Mbps.
Active LED	Off	There is no link to the Internet.
	On (green)	There is a link to the Internet.

Rear Panel

The rear panel of the wireless VPN firewall includes a cable lock receptacle, a console port, a Reset button, and a DC power connection.

Rear Panel

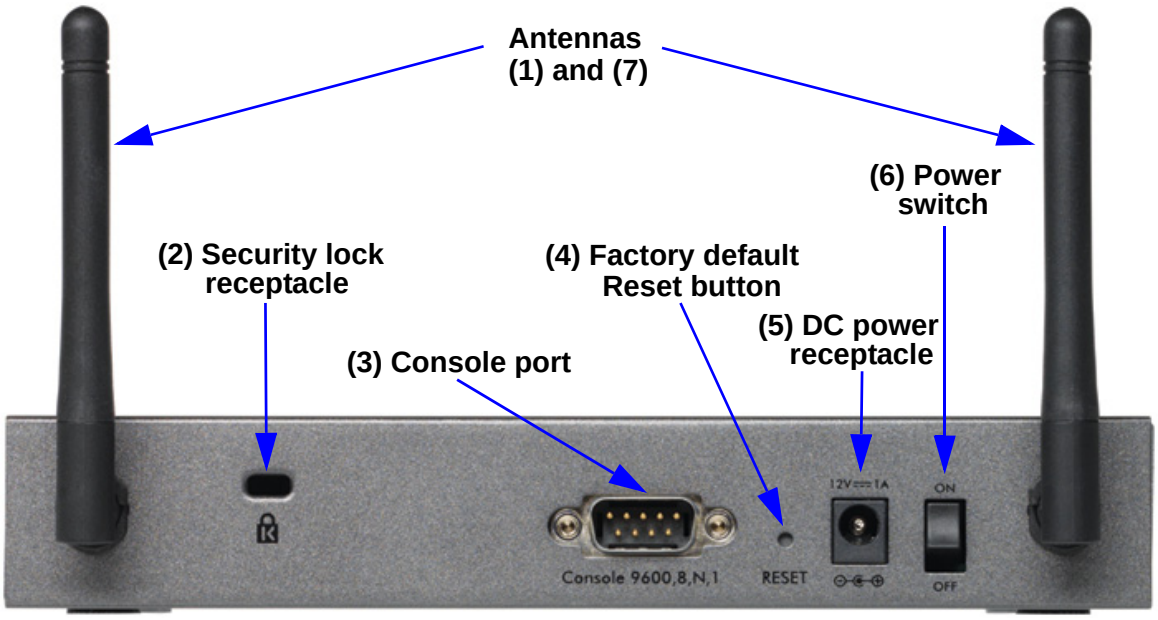


Figure 2.

Viewed from left to right, the rear panel contains the following components:

1. Detachable dipole antenna.
2. Cable security lock receptacle.
3. Console port. Port for connecting to an optional console terminal. The port has a DB9 male connector. The default baud rate is 9600 K. The pinouts are (2) Tx, (3) Rx, (5) and (7) Gnd.
4. Factory default Reset button. Using a sharp object, press and hold this button for about 8 seconds until the front panel Test LED flashes to reset the wireless VPN firewall to factory default settings. All configuration settings are lost, and the default password is restored.
5. DC power plug receptacle. Power input is 12VDC, 1A. The power plug is localized to the country of sale.
6. Power On/Off switch.
7. Detachable dipole antenna.

Bottom Panel with Product Label

The product label on the bottom of the wireless VPN firewall's enclosure displays factory defaults settings, regulatory compliance, and other information.

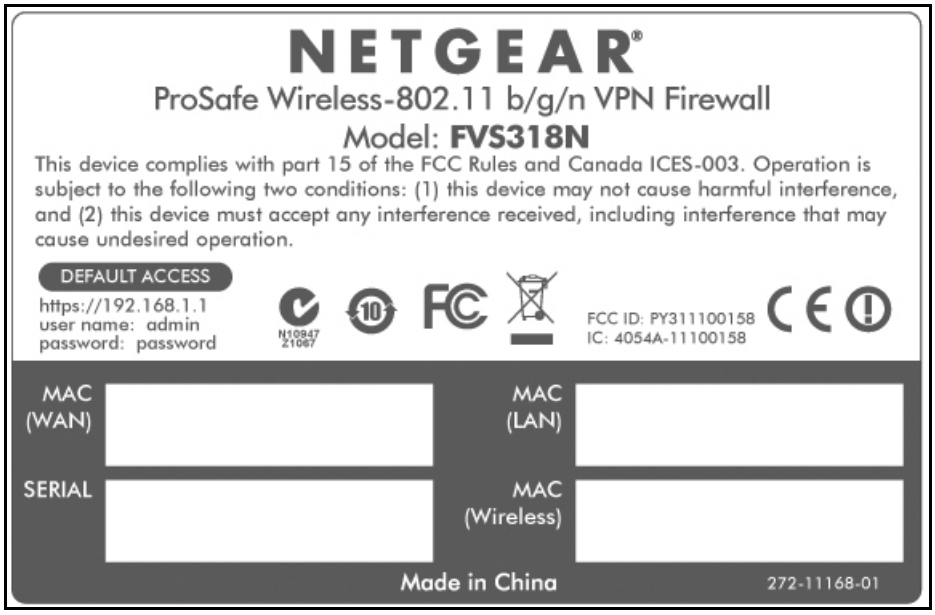

NETGEAR®
ProSafe Wireless-802.11 b/g/n VPN Firewall
Model: FVS318N
This device complies with part 15 of the FCC Rules and Canada ICES-003. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.
DEFAULT ACCESS
https://192.168.1.1
user name: admin
password: password
FCC ID: PY311100158
IC: 4054A-11100158
MAC (WAN)
MAC (LAN)
SERIAL
MAC (Wireless)
Made in China
272-11168-01

Figure 3.

Choose a Location for the Wireless VPN Firewall

The wireless VPN firewall is suitable for use in an office environment where it can be freestanding (on its runner feet) or mounted into a standard 19-inch equipment rack. Alternatively, you can rack-mount the wireless VPN firewall in a wiring closet or equipment room.

Consider the following when deciding where to position the wireless VPN firewall:

- The unit is accessible, and cables can be connected easily.
- Cabling is away from sources of electrical noise. These include lift shafts, microwave ovens, and air-conditioning units.
- Water or moisture cannot enter the case of the unit.
- Airflow around the unit and through the vents in the side of the case is not restricted. Provide a minimum of 25 mm or 1 inch clearance.
- The air is as free of dust as possible.
- Temperature operating limits are not likely to be exceeded. Install the unit in a clean, air-conditioned environment. For information about the recommended operating temperatures for the wireless VPN firewall, see *Appendix A, Default Settings and Technical Specifications*.

Internet and Broadband Settings

2

This chapter explains how to log in to the wireless VPN firewall, use the web management interface, configure the Internet and WAN settings, and configure the IPv6 settings. This chapter contains the following sections:

- *Log In to the Wireless VPN Firewall*
- *Internet and WAN Configuration Tasks*
- *Configure the IPv4 Internet Connection*
- *Configure the IPv6 Internet Connection*
- *Configure IPv6 Settings*
- *Configure Dynamic DNS*
- *Configure Advanced WAN Options and Other Tasks*
- *What to Do Next*

Note: To connect the wireless VPN firewall physically to your network, connect the cables and restart your network according to the instructions in the installation guide. See the *ProSafe Wireless-N 8-Port Gigabit VPN Firewall FVS318N Installation Manual* for complete steps. A PDF of the *Installation Guide* is on the NETGEAR support website.

Log In to the Wireless VPN Firewall

To configure the wireless VPN firewall, you need to use a web browser such as Microsoft Internet Explorer 6 or later, Mozilla Firefox 3 or later, or Apple Safari 3 or later with JavaScript, cookies, and SSL enabled.

Although these web browsers are qualified for use with the wireless VPN firewall's web management interface, SSL VPN users should choose a browser that supports JavaScript, Java, cookies, SSL, and ActiveX to take advantage of the full suite of applications. Note that Java is required only for the SSL VPN portal, not for the web management interface.

➢ **To connect and log in to the wireless VPN firewall:**

1. Start any of the qualified web browsers.
2. In the address field, enter **https://192.168.1.1**. The NETGEAR Configuration Manager Login screen displays in the browser.

Note: The wireless VPN firewall factory default IP address is 192.168.1.1. If you change the IP address, you need to use the IP address that you assigned to the wireless VPN firewall to log in to the wireless VPN firewall.

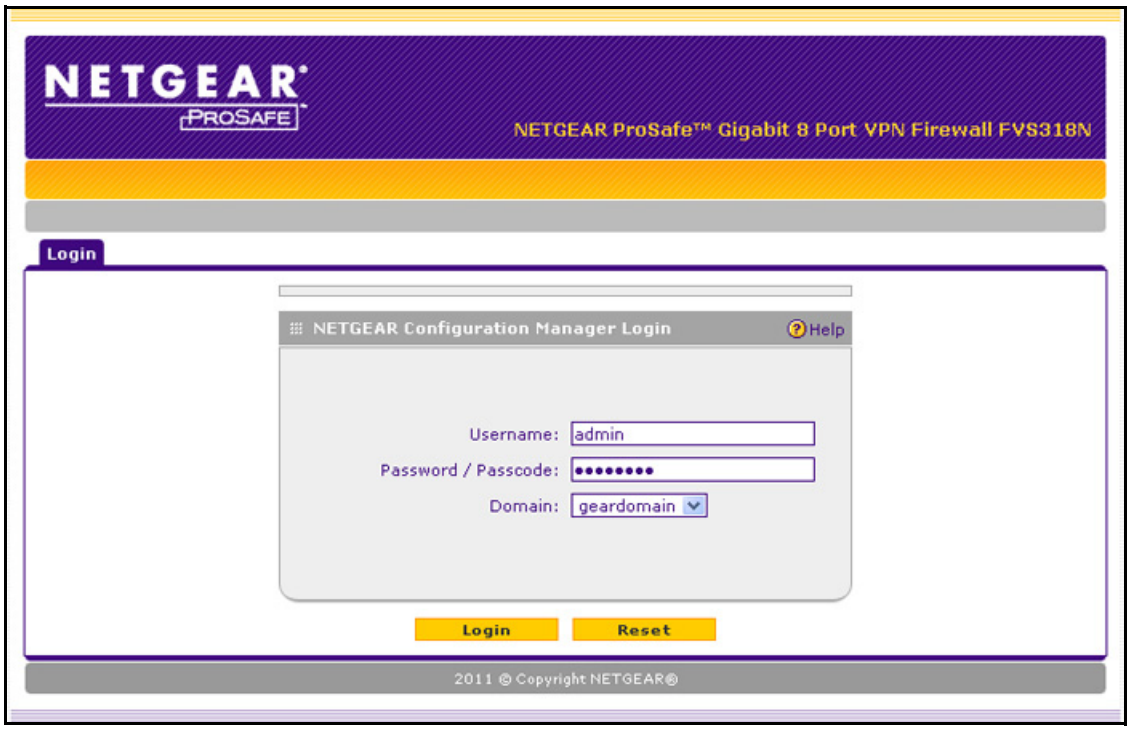


Figure 4.

3. In the User Name field, type **admin**. Use lowercase letters.
4. In the Password / Passcode field, type **password**. Here, too, use lowercase letters.

Note: The wireless VPN firewall user name and password are not the same as any user name or password you might use to log in to your Internet connection.

5. Click **Login**. The web management interface displays, showing the Router Status screen. The following figure shows the top part of the Router Status screen. For more information, see *View the System Status* on page 300.

Note: After 5 minutes of inactivity (the default login time-out), you are automatically logged out.

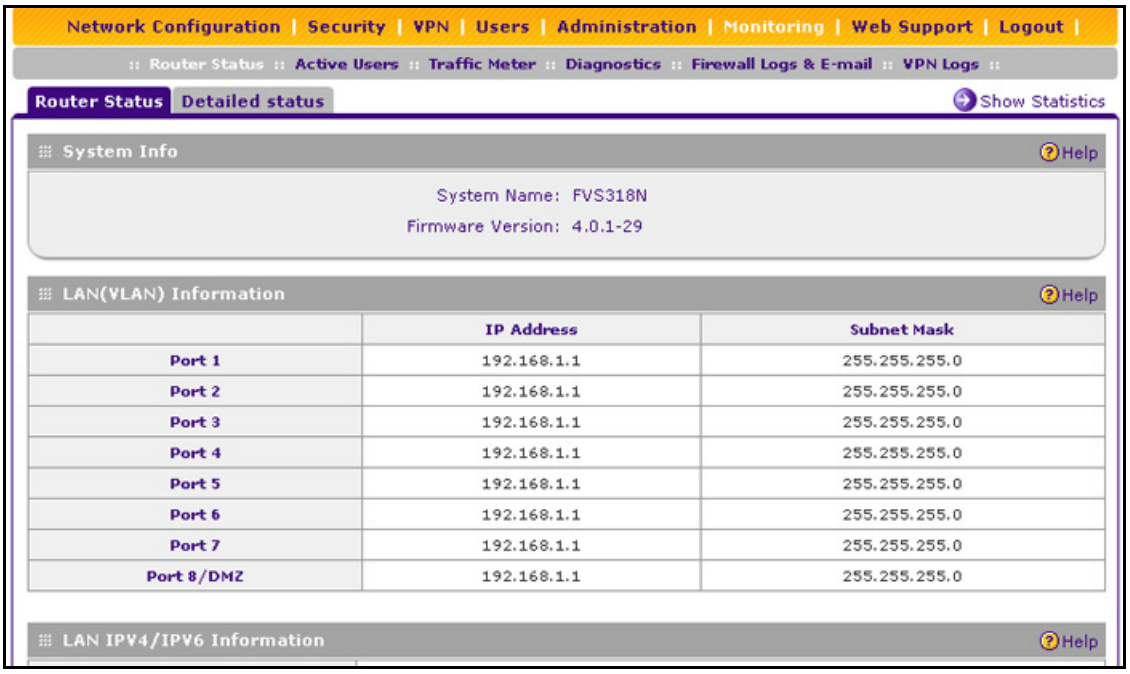

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Router Status :: Active Users :: Traffic Meter :: Diagnostics :: Firewall Logs & E-mail :: VPN Logs ::
Router Status
Detailed status
Show Statistics
System Info
Help
System Name: FVS318N
Firmware Version: 4.0.1-29
LAN(VLAN) Information
Help
IP Address
Subnet Mask
Port 1 192.168.1.1 255.255.255.0
Port 2 192.168.1.1 255.255.255.0
Port 3 192.168.1.1 255.255.255.0
Port 4 192.168.1.1 255.255.255.0
Port 5 192.168.1.1 255.255.255.0
Port 6 192.168.1.1 255.255.255.0
Port 7 192.168.1.1 255.255.255.0
Port 8/DMZ 192.168.1.1 255.255.255.0
LAN IPV4/IPV6 Information
Help

Figure 5.

Web Management Interface Menu Layout

The following figure shows the menu at the top the web management interface:

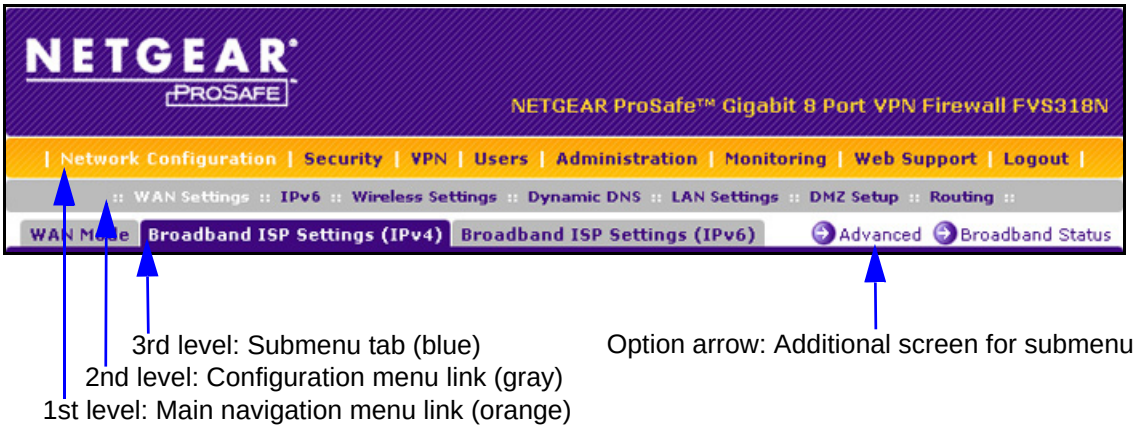

NETGEAR
PROSAFE
NETGEAR ProSafe™ Gigabit 8 Port VPN Firewall FVS318N
| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: IPv6 :: Wireless Settings :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing ::
Broadband ISP Settings (IPv4)
Broadband ISP Settings (IPv6)
Advanced
Broadband Status
3rd level: Submenu tab (blue)
2nd level: Configuration menu link (gray)
1st level: Main navigation menu link (orange)
Option arrow: Additional screen for submenu item

Figure 6.

The web management interface menu consists of the following components:

- **1st level: Main navigation menu links**. The main navigation menu in the orange bar across the top of the web management interface provides access to all the configuration functions of the wireless VPN firewall, and remains constant. When you select a main navigation menu link, the letters are displayed in white against an orange background.
- **2nd level: Configuration menu links**. The configuration menu links in the gray bar (immediately below the main navigation menu bar) change according to the main navigation menu link that you select. When you select a configuration menu link, the letters are displayed in white against a gray background.
- **3rd level: Submenu tabs**. Each configuration menu item has one or more submenu tabs that are listed below the gray menu bar. When you select a submenu tab, the text is displayed in white against a blue background.
- **Option arrows**. If there are additional screens for the submenu item, links to the screens display on the right side in blue letters against a white background, preceded by a white arrow in a blue circle.

The bottom of each screen provides action buttons. The nature of the screen determines which action buttons are shown. The following figure shows an example:

Figure 7.

Any of the following action buttons might display onscreen (this list might not be complete):

- **Apply**. Save and apply the configuration.
- **Reset**. Reset the configuration to default values.
- **Test**. Test the configuration before you decide whether or not to save and apply the configuration.
- **Auto Detect**. Enable the wireless VPN firewall to detect the configuration automatically and suggest values for the configuration.
- **Next**. Go to the next screen (for wizards).
- **Back**. Go to the previous screen (for wizards).
- **Cancel**. Cancel the operation.

When a screen includes a table, table buttons display to let you configure the table entries. The nature of the screen determines which table buttons are shown. The following figure shows an example:

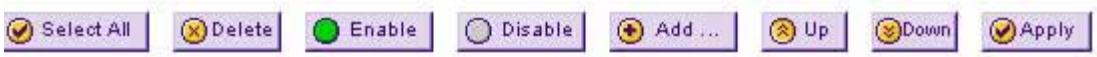


Figure 8.

Any of the following table buttons might display onscreen:

- **Select All**. Select all entries in the table.
- **Delete**. Delete the selected entry or entries from the table.

- **Enable**. Enable the selected entry or entries in the table.
- **Disable**. Disable the selected entry or entries in the table.
- **Add**. Add an entry to the table.
- **Edit**. Edit the selected entry.
- **Up**. Move the selected entry up in the table.
- **Down**. Move the selected entry down in the table.
- **Apply**. Apply the selected entry.

Almost all screens and sections of screens have an accompanying help screen. To open the help screen, click the (question mark) icon.

Requirements for Entering IP Addresses

To connect to the wireless VPN firewall, your computer needs to be configured to obtain an IP address automatically from the wireless VPN firewall, either an IPv4 address through DHCP or an IPv6 address through DHCPv6.

IPv4

The fourth octet of an IP address needs to be between 1 and 254 (both inclusive). This requirement applies to any IP address that you enter on a screen of the web management interface.

IPv6

IPv6 addresses are denoted by eight groups of hexadecimal quartets that are separated by colons. Any four-digit group of zeroes within an IPv6 address can be reduced to a single zero or altogether omitted.

The following errors invalidate an IPv6 address:

- More than eight groups of hexadecimal quartets
- More than four hexadecimal characters in a quartet
- More than two colons in a row

Internet and WAN Configuration Tasks

The tasks that are required to complete the Internet connection of your wireless VPN firewall depend on whether you use an IPv4 connection or an IPv6 connection to your Internet service provider (ISP).

Note: The wireless VPN firewall supports simultaneous IPv4 and IPv6 connections.

Set Up an IPv4 Internet Connection to Your ISP

➢ **Complete these four tasks:**

1. **Configure the Internet connections to your ISPs**. During this phase, you connect to your ISP. See *Configure the IPv4 Internet Connection* on page 24. You can also program the WAN traffic meter at this time if you wish. See *Enable the WAN Traffic Meter* on page 290.
2. **Configure the WAN mode**. Select either NAT or classical routing. See *Configure the IPv4 WAN Mode* on page 31.
3. **Configure Dynamic DNS on the WAN port (optional)**. Configure your fully qualified domain names during this phase (if required). See *Configure Dynamic DNS* on page 40.
4. **Configure the WAN options (optional)**. Optionally, you can enable each WAN port to respond to a ping, and you can change the factory default MTU size and port speed. However, these are advanced features, and changing them is not usually required. See *Configure Advanced WAN Options and Other Tasks* on page 43.

Each of these four tasks is detailed separately in this chapter.

Set Up an IPv6 Internet Connection to Your ISP

➢ **Complete these four tasks:**

1. **Configure the Internet connections to your ISPs**. During this phase, you connect to your ISP. See *Configure the IPv6 Internet Connection* on page 32. You can also program the WAN traffic meter at this time if you wish. See *Enable the WAN Traffic Meter* on page 290.
2. **Configure the IPv6 settings**. Select IPv4/IPv6 mode to support both IPv4 and IPv6 traffic and configure IPv6 tunnels. See *Configure IPv6 Settings* on page 36.
3. **Configure Dynamic DNS on the WAN port (optional)**. Configure your fully qualified domain names during this phase (if required). See *Configure Dynamic DNS* on page 40.
4. **Configure the WAN options (optional)**. Optionally, you can enable each WAN port to respond to a ping, and you can change the factory default MTU size and port speed. However, these are advanced features, and changing them is not usually required. See *Configure Advanced WAN Options and Other Tasks* on page 43.

Each of these four tasks is detailed separately in this chapter.

Configure the IPv4 Internet Connection

To set up your wireless VPN firewall for secure IPv4 Internet connections, you need to configure the WAN port. The web management interface offers two connection configuration options:

- Automatic detection and configuration of the network connection
- Manual configuration of the network connection

Each option is detailed in a section that follows.

Let the Wireless VPN Firewall Automatically Detect and Configure an IPv4 Internet Connection

➤ **To automatically configure the WAN port for an IPv4 connection to the Internet:**

1. Select **Network Configuration > WAN Settings > Broadband ISP Settings (IPv4)**. The ISP Broadband Settings (IPv4) screen displays:

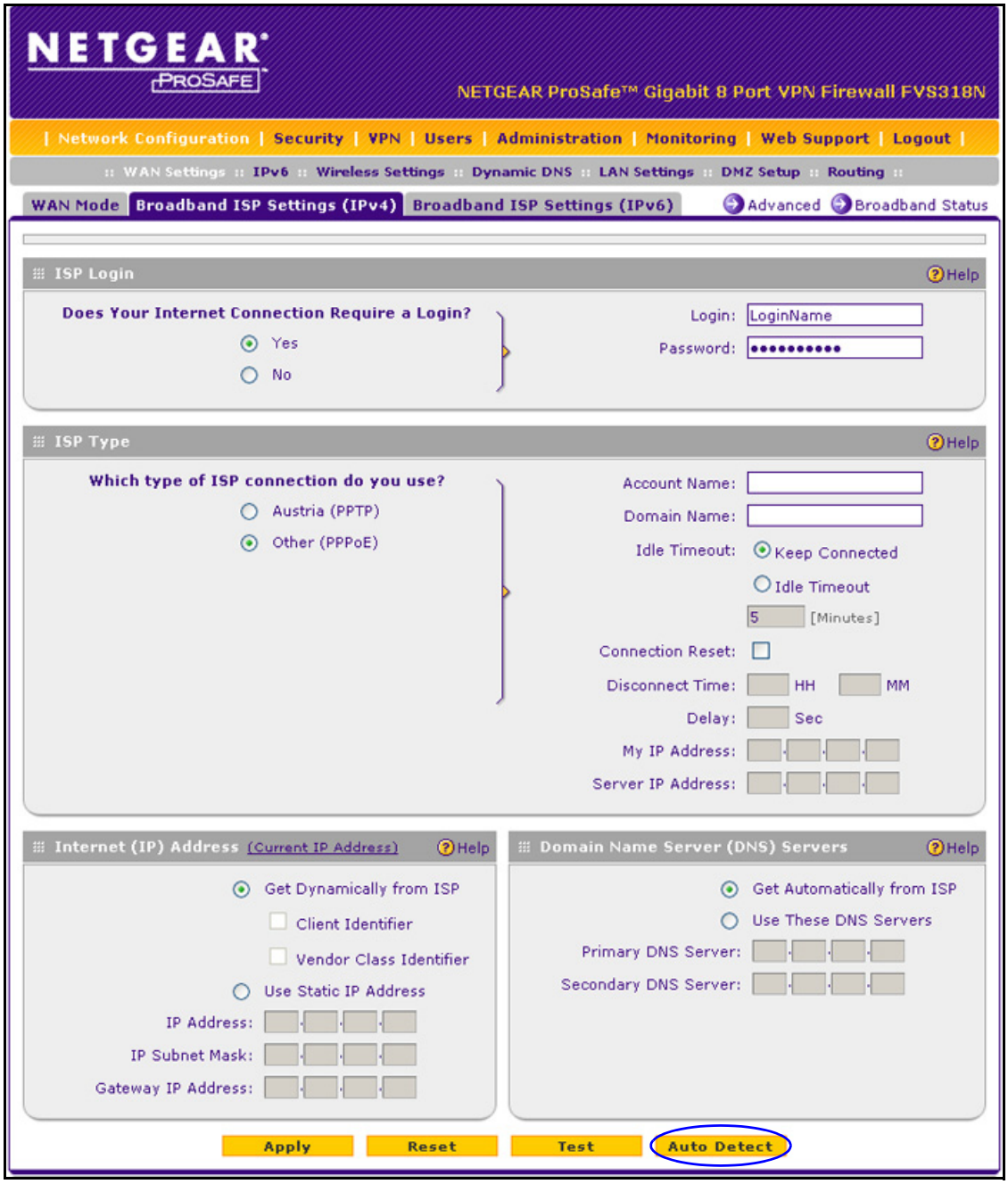


Figure 9.

2. Click the **Auto Detect** button at the bottom of the screen. The autodetect process probes the WAN port for a range of connection methods and suggests one that your ISP is most likely to support.

   The autodetect process returns one of the following results:

   - If the autodetect process is successful, a status bar at the top of the screen displays the results (for example, *DHCP service detected*).
   - If the autodetect process senses a connection method that requires input from you, it prompts you for the information. The following table explains the settings that you might have to enter:

     Table 2. Internet connection methods

Connection method	Manual data input required
DHCP (Dynamic IP)	No data is required.
PPPoE	The following fields are required: • Login • Password • Account Name • Domain Name
PPTP	The following fields are required: • Login • Password • Account Name • My IP Address • Server IP Address
Fixed (Static) IP	The following fields are required: • IP Address • IP Subnet Mask • Gateway IP Address

   - If the autodetect process does not find a connection, you are prompted either to check the physical connection between your wireless VPN firewall and the cable, DSL line, satellite dish, or wireless ISP radio antenna or to check your wireless VPN firewall's MAC address. For more information, see *Configure Advanced WAN Options and Other Tasks* on page 43 and *Troubleshoot the ISP Connection* on page 323.

3. To verify the connection, click the **Broadband Status** option arrow in the upper right of the screen to display the Connection Status pop-up screen. (The following figure shows a static IP address configuration.)

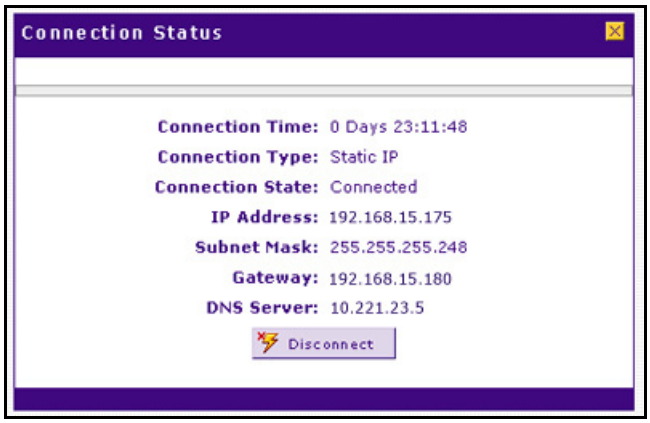


Figure 10.

The Connection Status screen should show a valid IP address and gateway, and you are connected to the Internet. If the configuration was not successful, skip ahead to *Manually Configure an IPv4 Internet Connection* on page 27, or see *Troubleshoot the ISP Connection* on page 323.

Note: For more information about the Connection Status screen, see *View the WAN Port Status* on page 311.

If the automatic WAN ISP configuration is successful, you can skip ahead to *Configure the IPv4 WAN Mode* on page 31.

Manually Configure an IPv4 Internet Connection

Unless your ISP automatically assigns your configuration through a DHCP server, you need to obtain configuration parameters from your ISP to manually establish an Internet connection. The required parameters for various connection types are listed in *Table 2* on page 26.

➢ **To manually configure the IPv4 broadband ISP settings:**

1. Select **Network Configuration > WAN Settings > Broadband ISP Settings (IPv4)**. The ISP Broadband Settings (IPv4) screen displays (see *Figure 9* on page 25).
2. Locate the IPS Login section on the screen:

Figure 11.

In the ISP Login section, select one of the following options:

- If your ISP requires an initial login to establish an Internet connection, select **Yes**. (The default is No.)
- If a login is not required, select **No**, and ignore the Login and Password fields.

3. If you selected Yes, enter the login name in the Login field and the password in the Password field. This information is provided by your ISP.
4. In the ISP Type section of the screen, select the type of ISP connection that you use from the two listed options. By default, Other (PPPoE) is selected, as shown in the following figure:

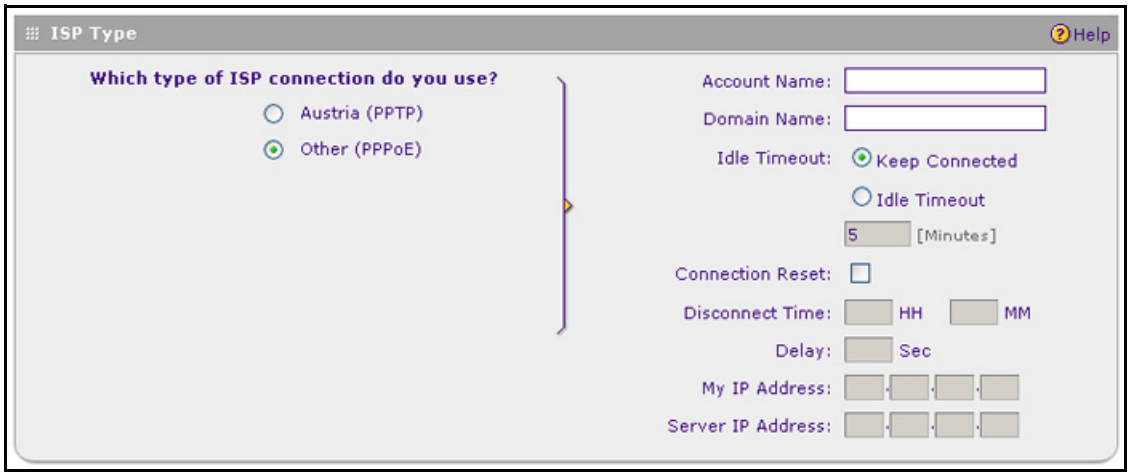


Figure 12.

5. If your connection is PPTP or PPPoE, your ISP requires an initial login. Enter the settings as explained in the following table:

Table 3. PPTP and PPPoE settings

Setting	Description	
Austria (PPTP)	If your ISP is Austria Telecom or any other ISP that uses PPTP for login, select this radio button, and enter the following settings:	
	Account Name	The account name is also known as the host name or system name. Enter the valid account name for the PPTP connection (usually your email ID assigned by your ISP). Some ISPs require you to enter your full email address here.
	Domain Name	Your domain name or workgroup name assigned by your ISP, or your ISP's domain name. You can leave this field blank.
	Idle Timeout	Select the **Keep Connected** radio button to keep the connection always on. To log out after the connection is idle for a period of time, select the **Idle Timeout** radio button and, in the time-out field, enter the number of minutes to wait before disconnecting. This is useful if your ISP charges you based on the period that you have logged in.

Table 3. PPTP and PPPoE settings (continued)

Setting	Description		
Austria (PPTP) (continued)	My IP Address	The IP address assigned by the ISP to make the connection with the ISP server.	
	Server IP Address	The IP address of the PPTP server.	
Other (PPPoE)	If you have installed login software, then your connection type is PPPoE. Select this radio button, and enter the following settings:		
	Account Name	The valid account name for the PPPoE connection.	
	Domain Name	The name of your ISP's domain or your domain name if your ISP has assigned one. You can leave this field blank.	
	Idle Timeout	Select the **Keep Connected** radio button to keep the connection always on. To log out after the connection is idle for a period of time, select the **Idle Timeout** radio button and, in the time-out field, enter the number of minutes to wait before disconnecting. This is useful if your ISP charges you based on the period that you have logged in.	
	Connection Reset	Select the **Connection Reset** check box to specify a time when the PPPoE WAN connection is reset, that is, the connection is disconnected momentarily and then reestablished. Then, specify the disconnect time and delay.	
		Disconnect Time	Specify the hour and minutes when the connection should be disconnected.
		Delay	Specify the period in seconds after which the connection should be reestablished.

6. In the Internet (IP) Address section of the screen (see the following figure), configure the IP address settings as explained in the following table. Click the **Current IP Address** link to see the currently assigned IP address.

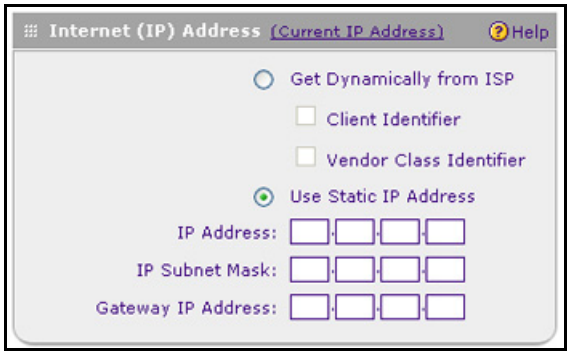


Table 4. Internet IP address settings

Setting	Description	
Get Dynamically from ISP	If your ISP has not assigned you a static IP address, select the **Get Dynamically from ISP** radio button. The ISP automatically assigns an IP address to the wireless VPN firewall using DHCP network protocol.	
	Client Identifier	If your ISP requires the client identifier information to assign an IP address using DHCP, select the **Client Identifier** check box.
	Vendor Class Identifier	If your ISP requires the vendor class identifier information to assign an IP address using DHCP, select the **Vendor Class Identifier** check box.
Use Static IP Address	If your ISP has assigned you a fixed (static or permanent) IP address, select the **Use Static IP Address** radio button, and enter the following settings:	
	IP Address	Static IP address assigned to you. This address identifies the wireless VPN firewall to your ISP.
	Subnet Mask	The subnet mask is usually provided by your ISP.
	Gateway IP Address	The IP address of the ISP's gateway is usually provided by your ISP.

7. In the Domain Name Server (DNS) Servers section of the screen (see the following figure), specify the DNS settings as explained in the following table.

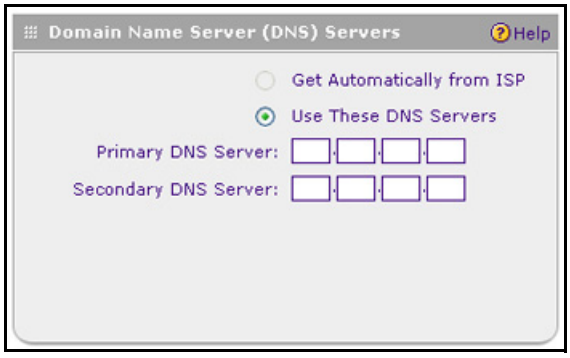


Figure 13.

Table 5. DNS server settings

Setting	Description	
Get Automatically from ISP	If your ISP has not assigned any Domain Name Server (DNS) addresses, select the **Get Automatically from ISP** radio button.	
Use These DNS Servers	If your ISP has assigned DNS addresses, select the **Use These DNS Servers** radio button. Make sure that you fill in valid DNS server IP addresses in the fields. Incorrect DNS entries might cause connectivity issues.	
	Primary DNS Server	The IP address of the primary DNS server.
	Secondary DNS Server	The IP address of the secondary DNS server.

8. Click **Test** to evaluate your entries. The wireless VPN firewall attempts to make a connection according to the settings that you entered.
9. Click **Apply** to save your changes.

Note: If your ISP requires MAC authentication and another MAC address has been previously registered with your ISP, then you need to enter that address on the Broadband Advanced Options screen for the corresponding WAN interface (see *Configure Advanced WAN Options and Other Tasks* on page 43).

Configure the IPv4 WAN Mode

Network Address Translation

Network Address Translation (NAT) allows all PCs on your LAN to share a single public Internet IP address. From the Internet, there is only a single device (the wireless VPN firewall) and a single IP address. PCs on your LAN can use any private IP address range, and these IP addresses are not visible from the Internet.

Note the following about NAT:

- The wireless VPN firewall uses NAT to select the correct PC (on your LAN) to receive any incoming data.
- If you have only a single public Internet IP address, you need to use NAT (the default setting).
- If your ISP has provided you with multiple public IP addresses, you can use one address as the primary shared address for Internet access by your PCs, and you can map incoming traffic on the other public IP addresses to specific PCs on your LAN. This one-to-one inbound mapping is configured using an inbound firewall rule.

Classical Routing

In classical routing mode, the wireless VPN firewall performs routing, but without NAT. To gain Internet access, each PC on your LAN needs to have a valid static Internet IP address.

If your ISP has allocated a number of static IP addresses to you, and you have assigned one of these addresses to each PC, you can choose classical routing. Or, you can use classical routing for routing private IP addresses within a campus environment.

To view the status of the WAN ports, you can view the Router Status screen (see *View the System Status* on page 300).

Configure the IPv4 Routing Mode

➢ **To configure the IPv4 routing mode:**

1. Select **Network Configuration > WAN Settings**. The WAN Mode screen displays.

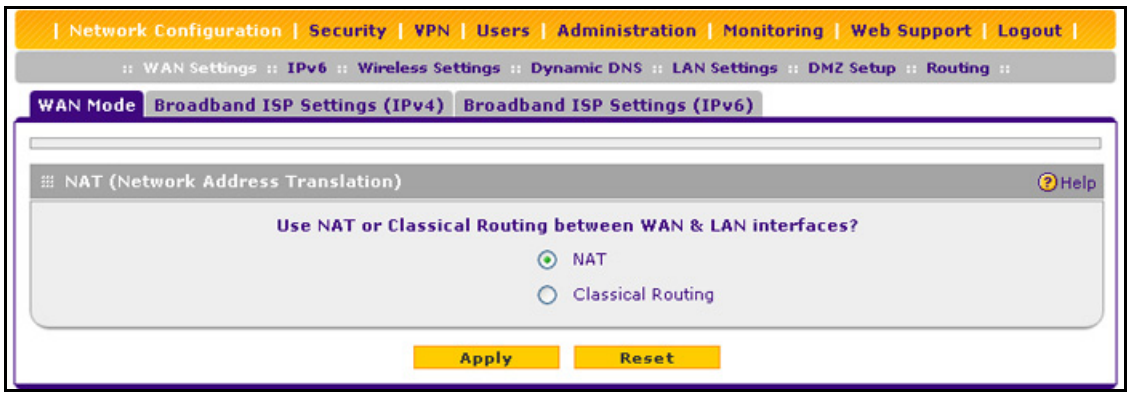

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
WAN Settings :: IPv6 :: Wireless Settings :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing
WAN Mode
Broadband ISP Settings (IPv4)
Broadband ISP Settings (IPv6)
NAT (Network Address Translation)
Help
Use NAT or Classical Routing between WAN & LAN interfaces?
NAT
Classical Routing
Apply
Reset

Figure 14.

2. Select the **NAT** radio button or the **Classical Routing** radio button.

WARNING!

Changing the WAN mode causes all LAN WAN and DMZ WAN inbound rules to revert to default settings.

3. Click **Apply** to save your settings.

Configure the IPv6 Internet Connection

To set up your wireless VPN firewall for secure IPv6 Internet connections, you need to configure the WAN port with a global unicast address. This is a public and routable IPv6 WAN address that can be statically or dynamically assigned. The web management interface offers two connection configuration options:

- Automatic configuration of the network connection.
- Manual configuration of the network connection

Each option is detailed in a section that follows.

Let the Wireless VPN Firewall Automatically Configure an IPv6 Internet Connection

The wireless VPN firewall can autoconfigure its ISP settings through a DHCPv6 server by using either stateless or stateful address autoconfiguration:

- **Stateless address autoconfiguration**. The wireless VPN firewall generates its own IP address by using a combination of locally available information and router advertisements, but receives DNS server information from a DHCP server.

  Router advertisements include a prefix that identifies the subnet that is associated with the WAN port. The IP address is formed by combining this prefix and the MAC address of the WAN port. The IP address is a dynamic address.

- **Stateful address autoconfiguration**. The wireless VPN firewall obtains an interface address, configuration information such as DNS server information, and other parameters from a DHCP server. The IP address is a dynamic address.

➢ **To automatically configure the WAN port for an IPv6 connection to the Internet:**

1. Select **Network Configuration > WAN Settings > Broadband ISP Settings (IPv6)**. The Broadband ISP Settings (IPv6) screen displays:

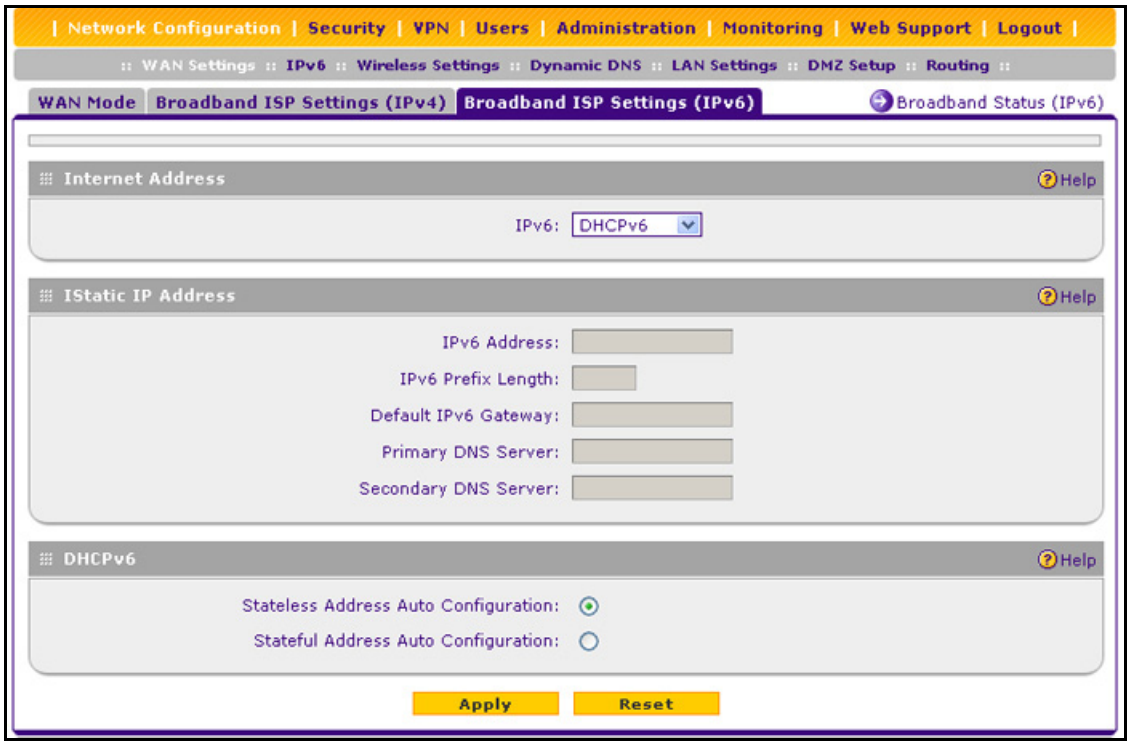


Figure 15.

2. In the Internet Address section of the screen, from the IPv6 drop-down list, select **DHCPv6**.

3. In the DHCPv6 section of the screen, select one of the following radio buttons:
   - **Stateless Address Auto Configuration**.
   - **Stateful Address Auto Configuration**.
4. Click **Apply** to save your changes.
5. To verify the connection, click the **Broadband Status (IPv6)** option arrow in the upper right of the screen to display the Connection Status pop-up screen. (The following figure shows a dynamic IP address configuration.)

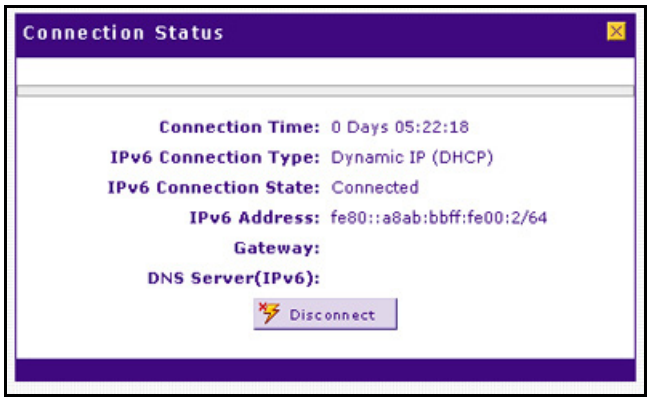


Figure 16.

The Connection Status screen should show a valid IP address and gateway, and you are connected to the Internet. If the configuration was not successful, see *Troubleshoot the ISP Connection* on page 323.

Note: For more information about the Connection Status screen, see *View the WAN Port Status* on page 311.

Manually Configure an IPv6 Internet Connection

To manually configure an IPv6 Internet connection, you need to receive static IP address information from your ISP.

➢ **To manually configure the IPv6 broadband ISP settings:**

1. Select **Network Configuration > WAN Settings > Broadband ISP Settings (IPv6)**. The Broadband ISP Settings (IPv6) screen displays:

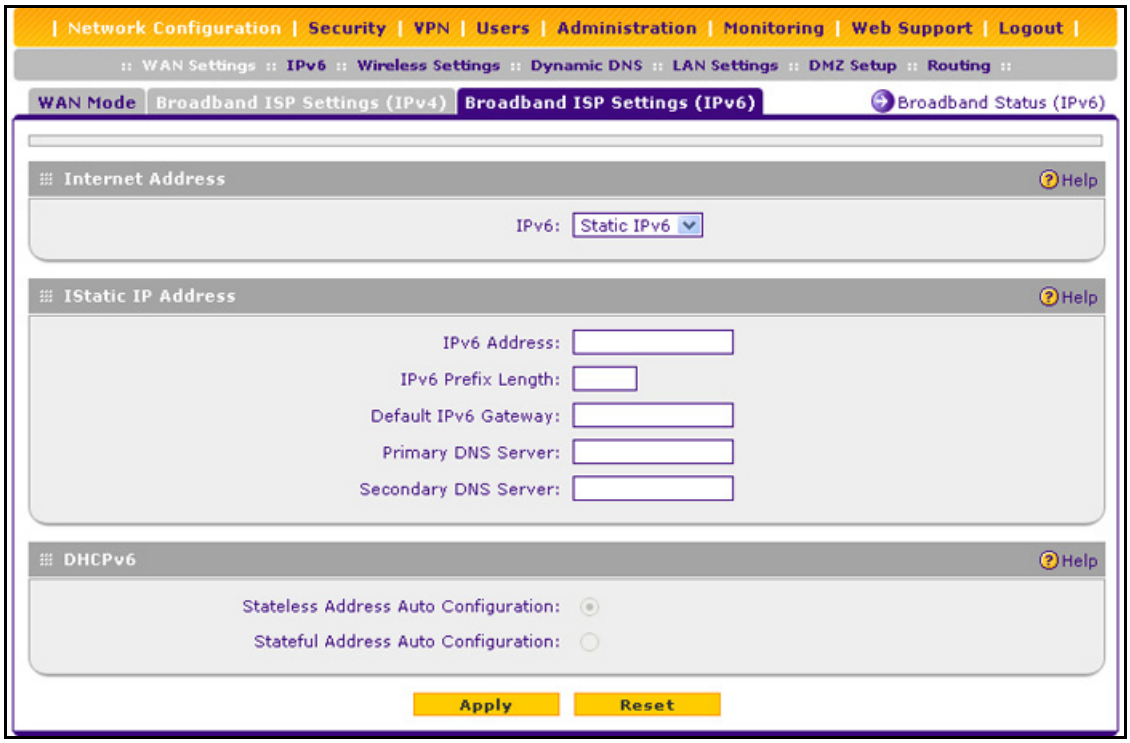


Figure 17.

2. In the Internet Address section of the screen, from the IPv6 drop-down list, select **Static IPv6**.
3. In the Static IP Address section of the screen, enter the settings as explained in the following table. You should have received static IPv6 address information from your ISP:

Table 6. Broadband ISP Settings (IPv6) screen settings

Setting	Description
IPv6 Address	The IP address in *one* of the following formats (all four examples specify the same IPv6 address): • 2001:DB8:0000:0000:020F:24FF:FEBF:DBCB • 2001:DB8:0:0:20F:24FF:FEBF:DBCB • 2001:DB8::20F24FF:FEBF:DBCB • 2001:DB8:0:0:20F:24FF:128:141:49:32
IPv6 Prefix Length	The prefix length, typically /64
Default IPv6 Gateway	The IPv6 IP address of the default IPv6 gateway
Primary DNS Server	The IPv6 IP address of the primary DNS server
Secondary DNS Server	The IPv6 IP address of the secondary DNS server

4. Click **Apply** to save your changes.

Note: If your ISP requires MAC authentication and another MAC address has been previously registered with your ISP, then you need to enter that address on the Broadband Advanced Options screen for the corresponding WAN interface (see *Configure Advanced WAN Options and Other Tasks* on page 43).

Configure IPv6 Settings

Because IPv4-only devices cannot communicate with IPv6-only devices (or the other way around) and IPv6 addresses are not yet very common, you need to specify if you want to restrict the wireless VPN firewall to support devices with IPv4 addresses only, or enable the wireless VPN firewall to support both devices with IPv4 addresses and devices with IPv6 addresses:

- **IPv4-only mode**. The wireless VPN firewall communicates only with devices that have IPv4 addresses, even though the wireless VPN firewall itself can have an IPv6 WAN address.
- **IPv4/IPv6 mode**. The wireless VPN firewall communicates with both devices that have IPv4 addresses and devices that have IPv6 addresses. IPv4/IPv6 mode is an IPv6-over-IPv4 mode in which IPv6 addresses are mapped to IPv4 addresses. You should configure tunnels to carry IPv6 packets over the existing IPv4 infrastructure (see *Configure IPv6 Tunnels* on page 37).

Configure the IPv6 Routing Mode

Note: IPv6 always functions in classical routing mode between the WAN interface and the LAN interfaces; NAT does not apply.

➢ **To configure the IPv6 routing mode:**

1. Select **Network Configuration > IPv6 > IP Mode**. The IP Mode screen displays:

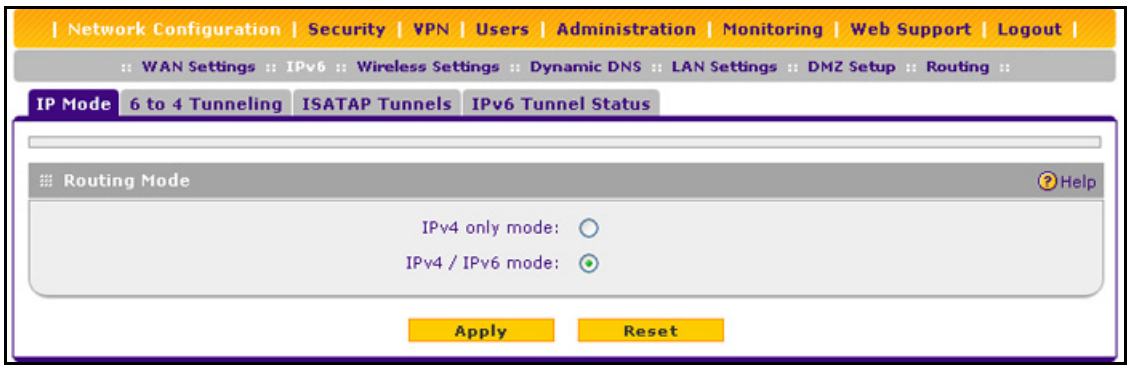


Figure 18.

2. Select one of the following radio buttons:
   - **IPv4 only mode**. This is the default mode.
   - **IPv4 / IPv6 mode**.

WARNING!

Changing the IP routing mode causes the wireless VPN firewall to reboot.

3. Click **Apply** to save your changes.

Configure IPv6 Tunnels

If you configure IPv4/IPv6 mode (see the previous section), tunnels are used to carry IPv6 packets over the existing IPv4 infrastructure. The wireless VPN firewall supports 6to4 and ISATAP tunnel mechanisms.

6to4 Tunnel Mechanism

6to4 is a WAN tunnel mechanism for automatic tunneling of IPv6 traffic between a device with an IPv6 address and a device with an IPv4 address, or the other way around. 6to4 tunneling is used to transfer IPv6 traffic between LAN IPv6 hosts and WAN IPv6 networks over the IPv4 network.

With 6to4 tunnels, IPv6 packets are embedded within the IPv4 packet and then transported over the IPv4 network. You do not need to specify tunnel endpoints, which are automatically determined by relay routers on the Internet. You cannot use 6to4 tunnels for traffic between IPv4-only devices and IPv6-only devices.

Typically, 6to4 tunnel addresses start with a 2002 prefix (decimal notification). On the wireless VPN firewall, a 6to4 tunnel is indicated by sit0-WAN1 (see *View the Tunnel Status* on page 40).

After you have enabled 6to4 tunneling, you need to enable the Router Advertisement Daemon (RADVD), add advertisement prefixes, and add static IPv6 routes.

To configure the wireless VPN firewall for 6to4 tunneling, follow the tasks that are presented in the following sections:

- *Configure 6to4 Tunneling* (following this section)
- *Configure the Router Advertisement Daemon and Advertisement Prefixes* on page 68
- *Manage Static IPv6 Routing* on page 81

Configure 6to4 Tunneling

➢ **To enable 6to4 automatic tunneling:**

1. Select **Network Configuration > IPv6 > 6 to 4 Tunneling**. The 6 to 4 Tunneling screen displays:

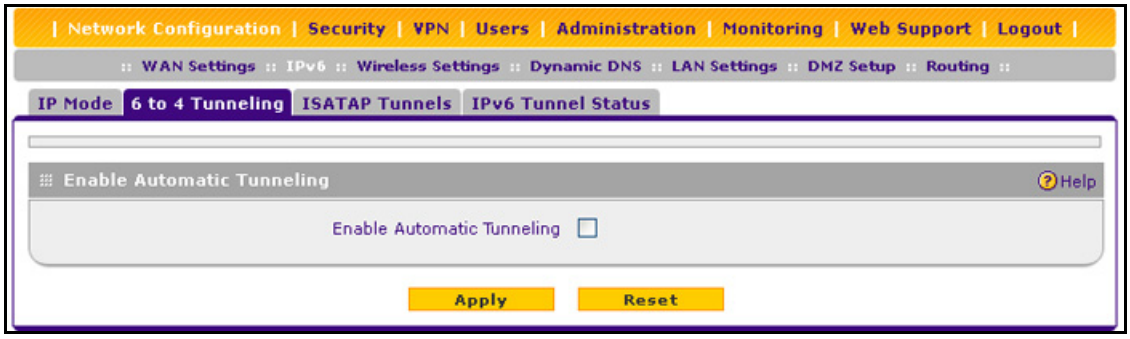


Figure 19.

2. Select the **Enable Automatic Tunneling** check box.
3. Click **Apply** to save your changes.

ISATAP Tunnel Mechanism

Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) is a LAN tunnel mechanism in which the IPv4 network functions as a virtual IPv6 local link. Each IPv4 address is mapped to a link-local IPv6 address, that is, the IPv4 address is used in the interface portion of the IPv6 address. For more information about link-local addresses, see *Configure IPv6 LAN Settings* on page 64.

The wireless VPN firewall determines the link-local address by concatenating the IPv6 address with the 32 bits of the IPv4 host address:

- For a unique global address: fe80:0000:0000:0000:0200:5efe (or fe80::200:5efe) is concatenated with the IPv4 address. For example, fe80::200:5efe with 10.29.33.4 becomes fe80::200:5efe:10.29.33.4, or in hexadecimal format, fe80::200:5efe:a1d:2104.
- For a private address: fe80:0000:0000:0000:0000:5efe (or fe80::5efe) is concatenated with the IPv4 address. For example, fe80::5efe with 192.168.1.1 becomes fe80::5efe:192.168.1.1, or in hexadecimal format, fe80::5efe:650a:6622.

Configure ISATAP Tunnels

➢ **To configure an ISATAP tunnel:**

1. Select **Network Configuration > IPv6 > ISATAP Tunnels**. The ISATAP Tunnels screen displays. (The following figure shows some examples.)

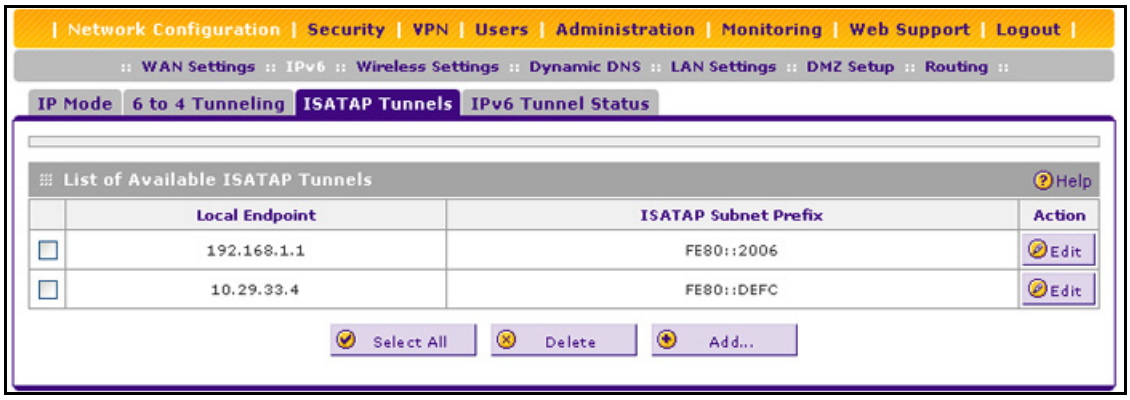


Figure 20.

2. Click the **Add** table button under the List of Available ISATAP Tunnels table. The Add ISATAP Tunnel screen displays:

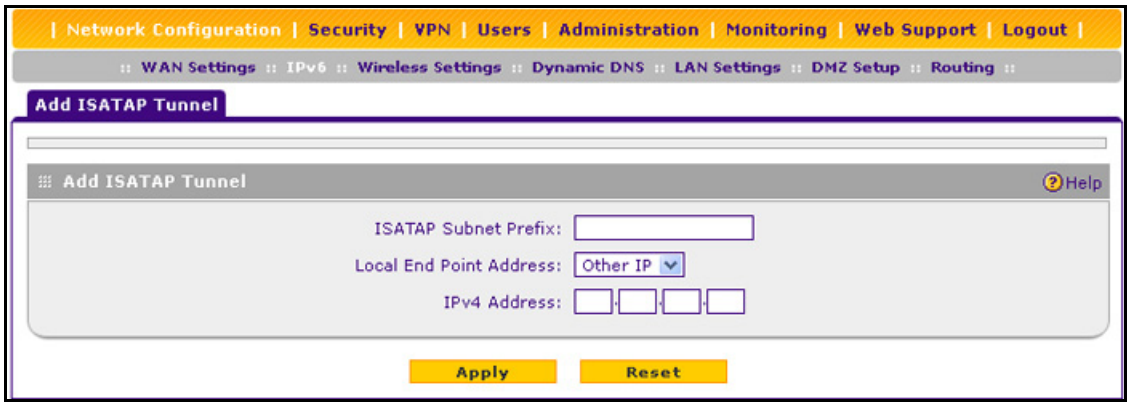

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
WAN Settings :: IPv6 :: Wireless Settings :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing
Add ISATAP Tunnel
Add ISATAP Tunnel
Help
ISATAP Subnet Prefix:
Local End Point Address:
Other IP
IPv4 Address:
Apply
Reset

Figure 21.

3. Specify the tunnel settings as explained in the following table.

Table 7. Add ISATAP Tunnel screen settings

Setting	Description
ISATAP Subnet Prefix	The IPv6 prefix for the tunnel.
Local End Point Address	From the drop-down list, select the type of local address: • **LAN**. The local end point address is the address of the default VLAN. • **Other IP**. The local end point address is another LAN IP address that you need to specify in the IPv4 Address fields.
IPv4 Address	If you selects Other IP from the Local End Point Address drop-down list, enter the IPv4 address.

4. Click **Apply** to save your changes.

➢ **To edit an ISATAP tunnel:**

1. On the ISATAP Tunnels screen, click the **Edit** button in the Action column for the tunnel that you want to modify. The Edit ISATAP Tunnel screen displays. This screen is identical to the Add ISATAP Tunnel screen.
2. Modify the settings as explained in the previous table.
3. Click **Apply** to save your settings.

➢ **To delete one or more tunnels:**

1. On the ISATAP Tunnels screen, select the check box to the left of each tunnel that you want to delete, or click the **Select All** table button to select all tunnels.
2. Click the **Delete** table button.

View the Tunnel Status

The IPv6 Tunnel Status screens displays the status of all active 6to4 and ISATAP tunnels.

➢ **To view the tunnel status:**

Select **Network Configuration > IPv6 > IPv6 Tunnel Status**. The IPv6 Tunnel Status screen displays:

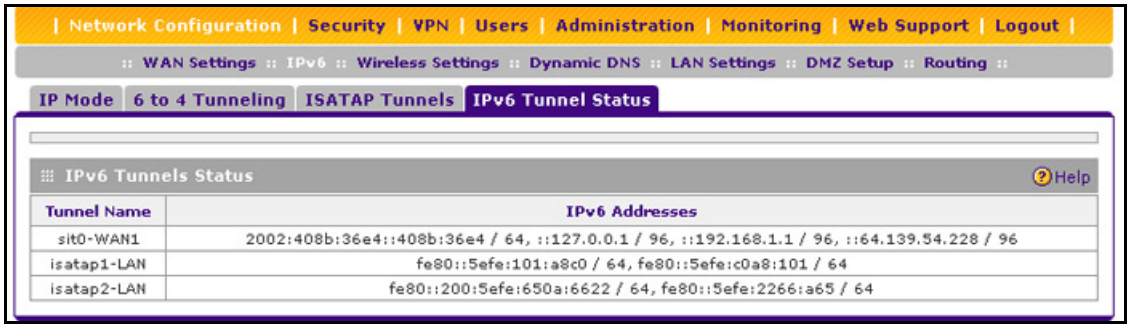

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
WAN Settings :: IPv6 :: Wireless Settings :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing
IP Mode
6 to 4 Tunneling
ISATAP Tunnels
IPv6 Tunnel Status
IPv6 Tunnels Status
Help
Tunnel Name
IPv6 Addresses
sit0-WAN1
2002:408b:36e4::408b:36e4 / 64, ::127.0.0.1 / 96, ::192.168.1.1 / 96, ::64.139.54.228 / 96
isatap1-LAN
fe80::5efe:101:a8c0 / 64, fe80::5efe:c0a8:101 / 64
isatap2-LAN
fe80::200:5efe:650a:6622 / 64, fe80::5efe:2266:a65 / 64

Figure 22.

The IPv6 Tunnel Status table shows the following fields:

- **Tunnel Name**. The tunnel name for the 6to4 tunnel is always sit0-WAN1 (SIT stands for simple Internet transition); the tunnel name for an ISATAP tunnel is isatapx-LAN, in which x is an integer.
- **IPv6 Address**. The IPv6 address of the local tunnel endpoint.

Configure Dynamic DNS

Dynamic DNS (DDNS) is an Internet service that allows devices with varying public IP addresses to be located using Internet domain names. To use DDNS, you need to set up an account with a DDNS provider such as DynDNS.org, TZO.com, Oray.net, or 3322.org. (Links to DynDNS, TZO, Oray, and 3322 are provided for your convenience as option arrows on the

DDNS configuration screens.) The wireless VPN firewall firmware includes software that notifies DDNS servers of changes in the WAN IP address so that the services running on this network can be accessed by others on the Internet.

If your network has a permanently assigned IP address, you can register a domain name and have that name linked with your IP address by public Domain Name Servers (DNS). However, if your Internet account uses a dynamically assigned IP address, you will not know in advance what your IP address will be, and the address can change frequently—hence, the need for a commercial DDNS service, which allows you to register an extension to its domain, and restores DNS requests for the resulting fully qualified domain name (FQDN) to your frequently changing IP address.

After you have configured your account information on the wireless VPN firewall, when your ISP-assigned IP address changes, your wireless VPN firewall automatically contacts your DDNS service provider, logs in to your account, and registers your new IP address.

Note: If your ISP assigns a private WAN IP address such as 192.168.x.x or 10.x.x.x, the DDNS service does not work because private addresses are not routed on the Internet.

➢ **To configure DDNS:**

1. Select **Network Configuration > Dynamic DNS**. The Dynamic DNS screen displays (see the following figure).
2. Click the submenu tab for your DDNS service provider:
   - **Dynamic DNS** for DynDNS.org (which is shown in the following figure)
   - **DNS TZO** for TZO.com
   - **DNS Oray** for Oray.net
   - **3322 DDNS** for 3322.org

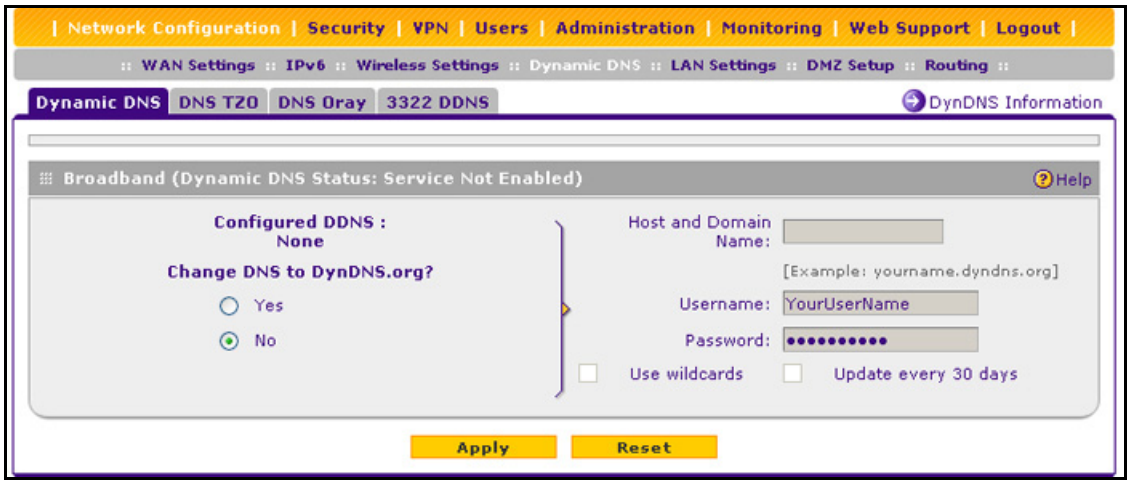


Figure 23.

3. Click the **Information** option arrow in the upper right of a DNS screen for registration information.

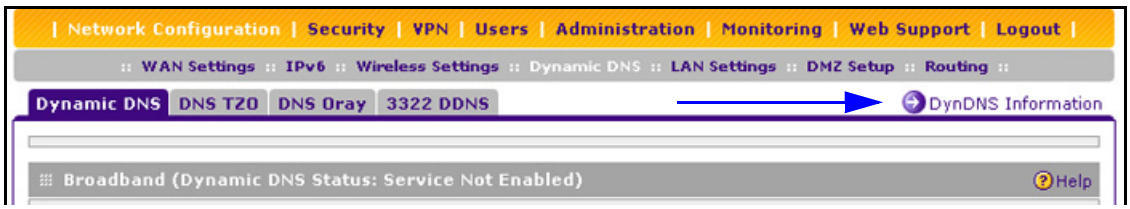

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
WAN Settings :: IPv6 :: Wireless Settings :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing
Dynamic DNS
DNS TZO
DNS Oray
3322 DDNS
DynDNS Information
Broadband (Dynamic DNS Status: Service Not Enabled)
Help

Figure 24.

4. Access the website of the DDNS service provider, and register for an account (for example, for DynDNS.org, go to *http://www.dyndns.com/*).
5. Configure the DDNS service settings as explained in the following table:

Table 8. DDNS service settings

Setting	Description	
Change DNS to (DynDNS, TZO, Oray, or 3322)	Select the **Yes** radio button to enable the DDNS service. The fields that display on the screen depend on the DDNS service provider that you have selected. Enter the following settings:	
	Host and Domain Name	The host and domain name for the DDNS service.
	Username or User Email Address	The user name or email address for DDNS server authentication.
	Password or User Key	The password that is used for DDNS server authentication.
	Use wildcards	If your DDNS provider allows the use of wildcards in resolving your URL, you can select the **Use wildcards** check box to activate this feature. For example, the wildcard feature causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org.
	Update every 30 days	If your WAN IP address does not change often, you might need to force a periodic update to the DDNS service to prevent your account from expiring. If the **Update every 30 days** check box displays, select it to enable a periodic update.

6. Click **Apply** to save your configuration.

Configure Advanced WAN Options and Other Tasks

The advanced options include configuring the maximum transmission unit (MTU) size, port speed, wireless VPN firewall's MAC address, and setting a rate limit on the traffic that is being forwarded by the wireless VPN firewall.

Note: Although you can access the Broadband Advanced Options screen only through the Broadband ISP Settings (IPv4) screen, the advanced options apply to both IPv4 and IPv6 WAN connections.

➢ **To configure advanced WAN options:**

1. Select **Network Configuration > WAN Settings > Broadband ISP Settings (IPv4)**. The Broadband ISP Settings (IPv4) screen displays (see *Figure 9* on page 25).
2. Click the **Advanced** option arrow in the upper right of the screen. The Broadband Advanced Options screen displays:

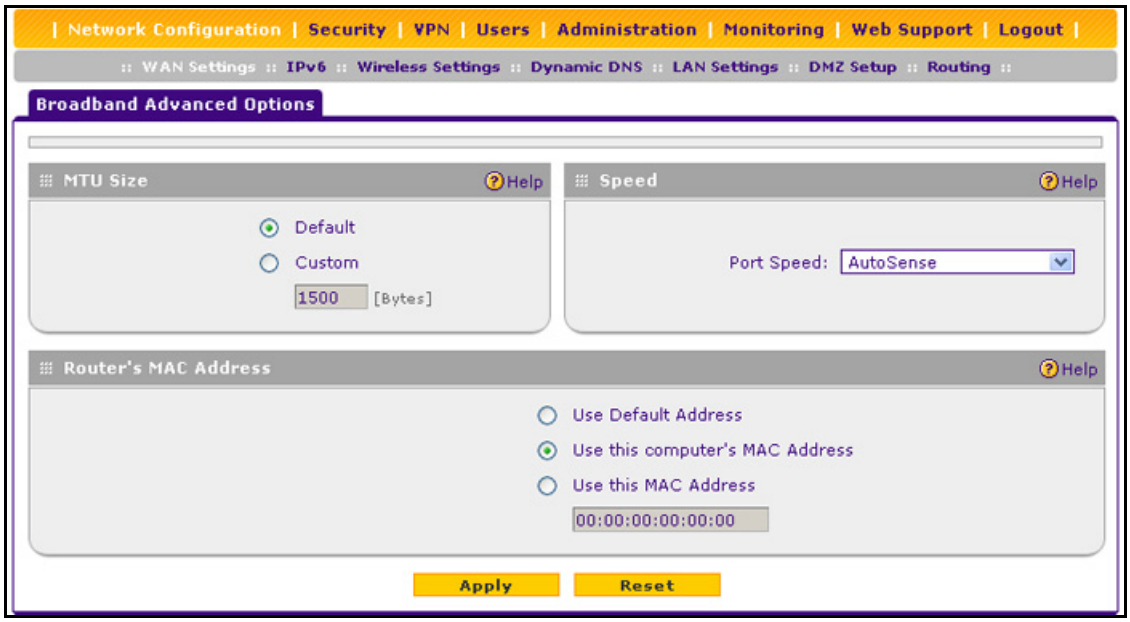


Figure 25.

3. Enter the settings as explained in the following table:

Table 9. Broadband Advanced Options screen settings

Setting	Description
MTU Size Make one of the following selections:	
Default	Select the **Default** radio button for the normal maximum transmit unit (MTU) value. For most Ethernet networks this value is 1500 bytes, or 1492 bytes for PPPoE connections.
Custom	Select the **Custom** radio button, and enter an MTU value in the Bytes field. For some ISPs, you might need to reduce the MTU. This is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.
Speed	
In most cases, the wireless VPN firewall can automatically determine the connection speed of the WAN port of the device (modem or router) that provides the WAN connection. If you cannot establish an Internet connection, you might need to manually select the port speed. If you know the Ethernet port speed of the modem or router, select it from the drop-down list. Use the half-duplex settings only if the full-duplex settings do not function correctly. Select one of the following speeds from the drop-down list: • **AutoSense**. Speed autosensing. This is the default setting, which can sense all Ethernet speeds and duplex modes, including 1000BASE-T speed at full duplex. • **10BaseT Half_Duplex**. Ethernet speed at half duplex. • **10BaseT Full_Duplex**. Ethernet speed at full duplex. • **100BaseT Half_Duplex**. Fast Ethernet speed at half duplex. • **100BaseT Full_Duplex**. Fast Ethernet speed at full duplex. • **1000BaseT Full_Duplex**. Gigabit Ethernet.	
Router's MAC Address Each computer or router on your network has a unique 48-bit local Ethernet address. This is also referred to as the computer's Media Access Control (MAC) address. The default is set to Use Default Address. Make one of the following selections:	
Use Default Address	Each computer or router on your network has a unique 32-bit local Ethernet address. This is also referred to as the computer's Media Access Control (MAC) address. To use the wireless VPN firewall's own MAC address, select the **Use Default Address** radio button.
Use this computer's MAC Address	Select the **Use this computer's MAC Address** radio button to allow the wireless VPN firewall to use the MAC address of the computer you are now using to access the web management interface. This setting is useful if your ISP requires MAC authentication.
Use this MAC Address	Select the **Use this MAC Address** radio button, and manually enter the MAC address in the field next to the radio button. You would typically enter the MAC address that your ISP is requiring for MAC authentication. **Note:** The format for the MAC address is 01:23:45:67:89:AB (numbers 0–9 and either uppercase or lowercase letters A–F). If you enter a MAC address, the existing entry is overwritten.

4. Click **Apply** to save your changes.

Additional WAN-Related Configuration Tasks

- If you want the ability to manage the wireless VPN firewall remotely, enable remote management (see *Configure Remote Management Access* on page 278). If you enable remote management, NETGEAR strongly recommends that you change your password (see *Change Passwords and Administrator and Guest Settings* on page 276).
- You can set up the traffic meter for the WAN interface, if you wish. See *Enable the WAN Traffic Meter* on page 290.

Verify the Connection

Test the wireless VPN firewall before deploying it in a live production environment. Verify that network traffic can pass through the wireless VPN firewall:

- Ping an Internet URL.
- Ping the IP address of a device on either side of the wireless VPN firewall.

What to Do Next

You have completed setting up the WAN connection for the wireless VPN firewall. The following chapters and sections describe important tasks that you need to address before you deploy the wireless VPN firewall in your network:

- *Chapter 3, LAN Configuration*
- *Chapter 4, Wireless Configuration and Security*
- *Configure Authentication Domains, Groups, and Users*
- *Manage Digital Certificates for VPN Connections*
- *Use the IPSec VPN Wizard for Client and Gateway Configurations*
- *Virtual Private Networking Using IPv4 SSL Connections*

LAN Configuration

3

This chapter describes how to configure the advanced LAN features of your wireless VPN firewall. This chapter contains the following sections:

- *Manage IPv4 Virtual LANs and DHCP Options*
- *Configure IPv4 Multihome LAN IP Addresses on the Default VLAN*
- *Manage IPv4 Groups and Hosts (IPv4 LAN Groups)*
- *Configure IPv6 LAN Settings*
- *Configure and Enable the DMZ Port for IPv4 Traffic*
- *Manage Static IPv4 Routing*
- *Manage Static IPv6 Routing*

Manage IPv4 Virtual LANs and DHCP Options

A local area network (LAN) can generally be defined as a broadcast domain. Hubs, bridges, or switches in the same physical segment or segments connect all end node devices. Endpoints can communicate with each other without the need for a router. Routers connect LANs together, routing the traffic to the appropriate port.

A virtual LAN (VLAN) is a local area network with a definition that maps workstations on some basis other than geographic location (for example, by department, type of user, or primary application). To enable traffic to flow between VLANs, traffic needs to go through a router, just as if the VLANs were on two separate LANs.

A VLAN is a group of PCs, servers, and other network resources that behave as if they were connected to a single network segment—even though they might not be. For example, all marketing personnel might be spread throughout a building. Yet if they are all assigned to a single VLAN, they can share resources and bandwidth as if they were connected to the same segment. The resources of other departments can be invisible to the marketing VLAN members, accessible to all, or accessible only to specified individuals, depending on how the IT manager has set up the VLANs.

VLANs have a number of advantages:

- It is easy to set up network segmentation. Users who communicate most frequently with each other can be grouped into common VLANs, regardless of physical location. Each group's traffic is contained largely within the VLAN, reducing extraneous traffic and improving the efficiency of the whole network.
- They are easy to manage. The addition of nodes, as well as moves and other changes, can be dealt with quickly and conveniently from a management interface rather than from the wiring closet.
- They provide increased performance. VLANs free up bandwidth by limiting node-to-node and broadcast traffic throughout the network.
- They ensure enhanced network security. VLANs create virtual boundaries that can be crossed only through a router. So standard, router-based security measures can be used to restrict access to each VLAN.

Port-Based VLANs

The wireless VPN firewall supports port-based VLANs. Port-based VLANs help to confine broadcast traffic to the LAN ports. Even though a LAN port can be a member of more than one VLAN, the port can have only one VLAN ID as its port VLAN identifier (PVID). By default, all eight LAN ports of the wireless VPN firewall are assigned to the default VLAN, or VLAN 1. Therefore, by default, all eight LAN ports have the default PVID 1. However, you can assign another PVID to a LAN port by selecting a VLAN profile from the drop-down list on the LAN Setup screen.

After you have created a VLAN profile and assigned one or more ports to the profile, you need to enable the profile to activate it.

The wireless VPN firewall's default VLAN cannot be deleted. All untagged traffic is routed through the default VLAN (VLAN1), which you need to assign to at least one LAN port.

Note the following about VLANs and PVIDs:

- One physical port is assigned to at least one VLAN.
- One physical port can be assigned to multiple VLANs.
- When one port is assigned to multiple VLANs, the port is used as a trunk port to connect to another switch or router.
- When a port receives an untagged packet, this packet is forwarded to a VLAN based on the PVID.
- When a port receives a tagged packet, this packet is forwarded to a VLAN based on the ID that is extracted from the tagged packet.

When you create a VLAN profile, assign LAN ports to the VLAN, and enable the VLAN, the LAN ports that are members of the VLAN can send and receive both tagged and untagged packets. Untagged packets that enter these LAN ports are assigned to the default PVID 1; packets that leave these LAN ports with the same default PVID 1 are untagged. All other packets are tagged according to the VLAN ID that you assigned to the VLAN when you created the VLAN profile.

This is a typical scenario for a configuration with an IP phone that has two Ethernet ports, one of which is connected to the wireless VPN firewall, the other one to another device:

Packets coming from the IP phone to the wireless VPN firewall LAN port are tagged. Packets passing through the IP phone from the connected device to the wireless VPN firewall LAN port are untagged. When you assign the wireless VPN firewall LAN port to a VLAN, packets entering and leaving the port are tagged with the VLAN ID. However, untagged packets entering the wireless VPN firewall LAN port are forwarded to the default VLAN with PVID 1; packets that leave the LAN port with the same default PVID 1 are untagged.

Note: The configuration of the DHCP options for the default VLAN are explained in *Configure the IPv4 Internet Connection* on page 24. For information about how to add and edit a VLAN profile, including its DHCP options, see *Configure a VLAN Profile* on page 51.

Assign and Manage VLAN Profiles

➢ **To assign VLAN profiles to the LAN ports and manage VLAN profiles:**

1. Select **Network Configuration > LAN Settings**. The LAN submenu tabs display, with the LAN Setup (IPv4) screen in view. (The following figure contains some VLAN profiles as an example.)

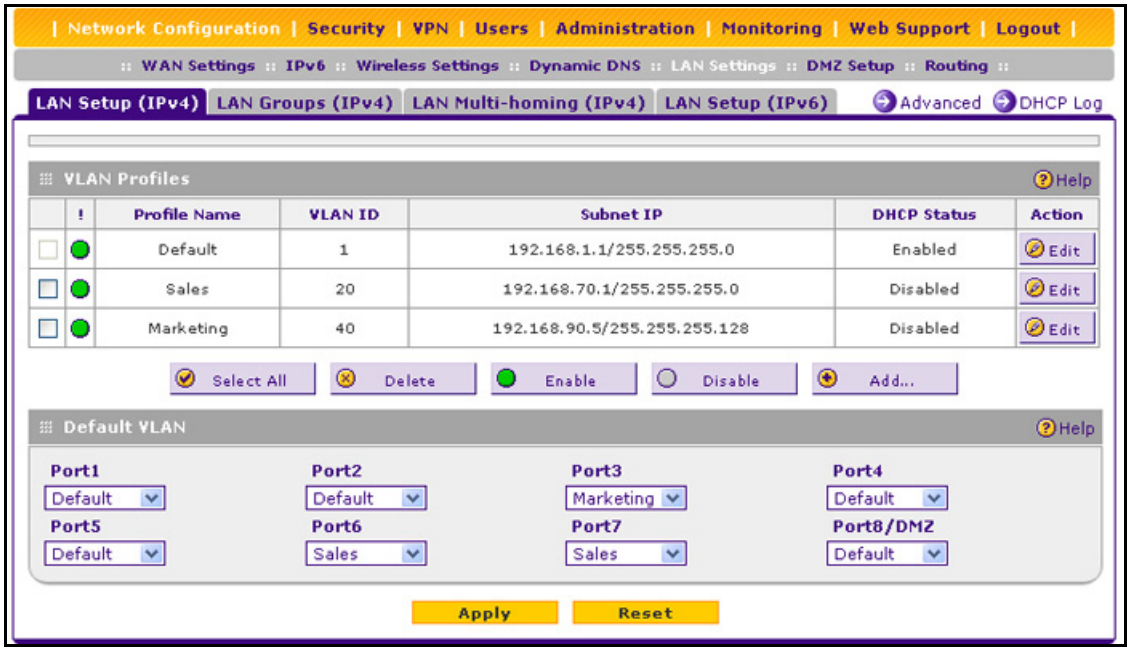

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
WAN Settings :: IPv6 :: Wireless Settings :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing
LAN Setup (IPv4) LAN Groups (IPv4) LAN Multi-homing (IPv4) LAN Setup (IPv6) Advanced DHCP Log
VLAN Profiles Help
! Profile Name VLAN ID Subnet IP DHCP Status Action
Default 1 192.168.1.1/255.255.255.0 Enabled Edit
Sales 20 192.168.70.1/255.255.255.0 Disabled Edit
Marketing 40 192.168.90.5/255.255.255.128 Disabled Edit
Select All Delete Enable Disable Add...
Default VLAN Help
Port1 Default
Port2 Default
Port3 Marketing
Port4 Default
Port5 Default
Port6 Sales
Port7 Sales
Port8/DMZ Default
Apply Reset

Figure 26.

For each VLAN profile, the following fields display in the VLAN Profiles table:

- **Check box**. Allows you to select the VLAN profile in the table.
- **Status icon**. Indicates the status of the VLAN profile:
  - **Green circle**. The VLAN profile is enabled.
  - **Gray circle**. The VLAN profile is disabled.
- **Profile Name**. The unique name assigned to the VLAN profile.
- **VLAN ID**. The unique ID (or tag) assigned to the VLAN profile.
- **Subnet IP**. The subnet IP address for the VLAN profile.
- **DHCP Status**. The DHCP server status for the VLAN profile, which can be either DHCP Enabled or DHCP Disabled.
- **Action**. The Edit table button, which provides access to the Edit VLAN Profile screen.

2. Assign a VLAN profile to a LAN port by selecting a VLAN profile from the drop-down list. Both enabled and disabled VLAN profiles are displayed in the drop-down lists.
3. Click **Apply** to save your settings.

VLAN DHCP Options

For each VLAN, you need to specify the Dynamic Host Configuration Protocol (DHCP) options (see *Configure a VLAN Profile* on page 51). The configuration of the DHCP options for the wireless VPN firewall's default VLAN, or VLAN 1, is explained in *Configure the IPv4 Internet Connection* on page 24. This section provides further information about the DHCP options.

DHCP Server

The default VLAN (VLAN 1) has the DHCP server option enabled by default, allowing the wireless VPN firewall to assign IP, DNS server, WINS server, and default gateway addresses to all computers connected to the wireless VPN firewall's LAN. The assigned default gateway address is the LAN address of the wireless VPN firewall. IP addresses are assigned to the attached computers from a pool of addresses that you need to specify. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN. When you create a new VLAN, the DHCP server option is disabled by default.

For most applications, the default DHCP server and TCP/IP settings of the wireless VPN firewall are satisfactory.

The wireless VPN firewall delivers the following settings to any LAN device that requests DHCP:

- An IP address from the range that you have defined
- Subnet mask
- Gateway IP address (the wireless VPN firewall's LAN IP address)
- Primary DNS server (the wireless VPN firewall's LAN IP address)
- WINS server (if you entered a WINS server address in the DHCP Setup screen)
- Lease time (the date obtained and the duration of the lease)

DHCP Relay

DHCP relay options allow you to make the wireless VPN firewall a DHCP relay agent for a VLAN. The DHCP relay agent makes it possible for DHCP broadcast messages to be sent over routers that do not support forwarding of these types of messages. The DHCP relay agent is therefore the routing protocol that enables DHCP clients to obtain IP addresses from a DHCP server on a remote subnet. If you do not configure a DHCP relay agent for a VLAN, its clients can obtain IP addresses only from a DHCP server that is on the same subnet. To enable clients to obtain IP addresses from a DHCP server on a remote subnet, you need to configure the DHCP relay agent on the subnet that contains the remote clients, so that the DHCP relay agent can relay DHCP broadcast messages to your DHCP server.

DNS Proxy

When the DNS proxy option is enabled for a VLAN, the wireless VPN firewall acts as a proxy for all DNS requests and communicates with the ISP's DNS servers (as configured on the Broadband ISP Settings screens). All DHCP clients receive the primary and secondary DNS IP addresses along with the IP address where the DNS proxy is located (that is, the wireless VPN firewall's LAN IP address). When the DNS proxy option is disabled for a VLAN, all DHCP clients receive the DNS IP addresses of the ISP but without the DNS proxy IP address.

LDAP Server

A Lightweight Directory Access Protocol (LDAP) server allows a user to query and modify directory services that run over TCP/IP. For example, clients can query email addresses, contact information, and other service information using an LDAP server. For each VLAN, you can specify an LDAP server and a search base that defines the location in the directory (that is, the directory tree) from which the LDAP search begins.

Configure a VLAN Profile

For each VLAN on the wireless VPN firewall, you can configure its profile, port membership, LAN TCP/IP settings, DHCP options, DNS server, and inter-VLAN routing capability.

➤ **To add a VLAN profile:**

1. Select **Network Configuration > LAN Settings**. The LAN submenu tabs display, with the LAN Setup (IPv4) screen in view. The following figure shows the LAN Setup (IPv4) screen with the default VLAN profile and two other VLAN profiles as an example.

Note: For information about how to manage VLANs, see *Port-Based VLANs* on page 47. The following information describes how to configure a VLAN profile.

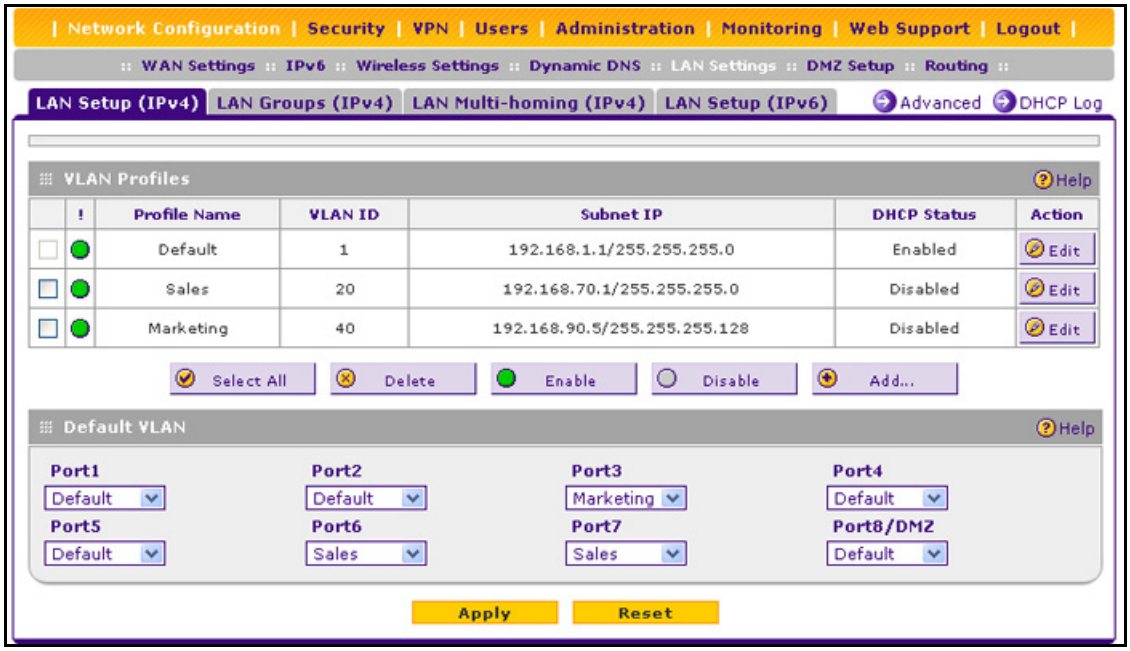

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
WAN Settings :: IPv6 :: Wireless Settings :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing
LAN Setup (IPv4) LAN Groups (IPv4) LAN Multi-homing (IPv4) LAN Setup (IPv6) Advanced DHCP Log
VLAN Profiles Help
! Profile Name VLAN ID Subnet IP DHCP Status Action
Default 1 192.168.1.1/255.255.255.0 Enabled Edit
Sales 20 192.168.70.1/255.255.255.0 Disabled Edit
Marketing 40 192.168.90.5/255.255.255.128 Disabled Edit
Select All Delete Enable Disable Add...
Default VLAN Help
Port1 Default
Port2 Default
Port3 Marketing
Port4 Default
Port5 Default
Port6 Sales
Port7 Sales
Port8/DMZ Default
Apply Reset

Figure 27.

2. Click the **Add** table button under the VLAN Profiles table. The Add VLAN Profile screen displays.

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
WAN Settings :: IPv6 :: Wireless Settings :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing
Add VLAN Profile
VLAN Profile
Help
Profile Name:
VLAN ID:
Port Membership
Help
Port 1
Port 2
Port 3
Port 4
Port 5
Port 6
Port 7
Port 8/DMZ
IP Setup
Help
IP Address:
Subnet Mask:
DHCP
Help
Disable DHCP Server
Enable DHCP Server
Enable LDAP information
Domain Name:
LDAP Server:
Start IP:
Search Base:
End IP:
Port:
(enter 0 for default port)
Primary DNS Server:
Secondary DNS Server:
WINS Server:
Lease Time:
Hours
DHCP Relay
Relay Gateway:
DNS Proxy
Help
Enable DNS Proxy:
Inter VLAN Routing
Help
Enable Inter VLAN Routing:
Apply
Reset

Figure 28.

3. Enter the settings as explained in the following table:

Table 10. Add VLAN Profile screen settings

Setting	Description
VLAN Profile	
Profile Name	Enter a unique name for the VLAN profile.
VLAN ID	Enter a unique ID number for the VLAN profile. No two VLANs can have the same VLAN ID number. **Note:** You can enter VLAN IDs from 2 to 4093. VLAN ID 1 is reserved for the default VLAN; VLAN ID 4094 is reserved for the DMZ interface.
Port Membership	
Port 1, Port 2, Port 3, Port 4, Port 5, Port 6, Port 7, and Port 8 / DMZ	Select one, several, or all port check boxes to make the ports members of this VLAN. **Note:** A port that is defined as a member of a VLAN profile can send and receive data frames that are tagged with the VLAN ID.
IP Setup	
IP Address	Enter the IP address of the wireless VPN firewall (the factory default address is 192.168.1.1). **Note:** Always make sure that the LAN port IP address and DMZ port IP address are in different subnets. **Note:** If you change the LAN IP address of the VLAN while being connected through the browser to the VLAN, you are disconnected. You then need to open a new connection to the new IP address and log in again. For example, if you change the default IP address 192.168.1.1 to 10.0.0.1, you now need to enter **https://10.0.0.1** in your browser to reconnect to the web management interface.
Subnet Mask	Enter the IP subnet mask. The subnet mask specifies the network number portion of an IP address. Based on the IP address that you assign, the wireless VPN firewall automatically calculates the subnet mask. Unless you are implementing subnetting, use 255.255.255.0 as the subnet mask (computed by the wireless VPN firewall).
DHCP	
Disable DHCP Server	If another device on your network is the DHCP server for the VLAN, or if you will manually configure the network settings of all of your computers, select the **Disable DHCP Server** radio button to disable the DHCP server. This is the default setting.

Table 10. Add VLAN Profile screen settings (continued)

Setting	Description	
Enable DHCP Server	Select the **Enable DHCP Server** radio button to enable the wireless VPN firewall to function as a Dynamic Host Configuration Protocol (DHCP) server, providing TCP/IP configuration for all computers connected to the VLAN. Enter the following settings:	
	Domain Name	This setting is optional. Enter the domain name of the wireless VPN firewall.
	Start IP Address	Enter the start IP address. This address specifies the first of the contiguous addresses in the IP address pool. Any new DHCP client joining the LAN is assigned an IP address between this address and the end IP address.
	End IP Address	Enter the end IP address. This address specifies the last of the contiguous addresses in the IP address pool. Any new DHCP client joining the LAN is assigned an IP address between the start IP address and this IP address. **Note:** The start and end DHCP IP addresses should be in the same *network* as the LAN IP address of the wireless VPN firewall (that is, the IP address in the IP Setup section as described earlier in this table).
	Primary DNS Server	This setting is optional. If an IP address is specified, the wireless VPN firewall provides this address as the primary DNS server IP address. If no address is specified, the wireless VPN firewall uses the VLAN IP address as the primary DNS server IP address.
	Secondary DNS Server	This setting is optional. If an IP address is specified, the wireless VPN firewall provides this address as the secondary DNS server IP address.
	WINS Server	This setting is optional. Enter a WINS server IP address to specify the Windows NetBIOS server, if one is present in your network.
	Lease Time	Enter a lease time. This specifies the duration for which IP addresses are leased to clients.
DHCP Relay	To use the wireless VPN firewall as a DHCP relay agent for a DHCP server somewhere else in your network, select the **DHCP Relay** radio button. Enter the following setting:	
	Relay Gateway	The IP address of the DHCP server for which the wireless VPN firewall serves as a relay.

Table 10. Add VLAN Profile screen settings (continued)

Setting	Description	
Enable LDAP information	To enable the DHCP server to provide Lightweight Directory Access Protocol (LDAP) server information, select the **Enable LDAP information** check box. Enter the following settings.	
	LDAP Server	The IP address or name of the LDAP server.
	Search Base	The search objects that specify the location in the directory tree from which the LDAP search begins. You can specify multiple search objects, separated by commas. The search objects include: • CN (for common name) • OU (for organizational unit) • O (for organization) • C (for country) • DC (for domain) For example, to search the Netgear.net domain for all last names of Johnson, you would enter: cn=Johnson,dc=Netgear,dc=net
	Port	The port number for the LDAP server. The default setting is 0 (zero).
DNS Proxy		
Enable DNS Proxy	This setting is optional. To enable the wireless VPN firewall to provide a LAN IP address for DNS address name resolution, select the **Enable DNS Proxy** check box. This setting is disabled by default. **Note:** When the DNS proxy option is disabled for a VLAN, all DHCP clients receive the DNS IP addresses of the ISP but without the DNS proxy IP address.	
Inter VLAN Routing		
Enable Inter VLAN Routing	This setting is optional. To ensure that traffic is routed only to VLANs for which inter-VLAN routing is enabled, select the **Enable Inter VLAN Routing** check box. This setting is disabled by default. When the Enable Inter VLAN Routing check box is not selected, traffic from this VLAN is not routed to other VLANs, and traffic from other VLANs is not routed to this VLAN.	

4. Click **Apply** to save your settings.

Note: Once you have completed the LAN setup, all outbound traffic is allowed and all inbound traffic is discarded except responses to requests from the LAN side. For information about how to change these default traffic rules, see *Chapter 5, IPv4 Firewall Protection*.

➢ **To edit a VLAN profile:**

1. On the LAN Setup (IPv4) screen (see *Figure 27* on page 51), click the **Edit** button in the Action column for the VLAN profile that you want to modify. The Edit VLAN Profile screen displays. This screen is identical to the Add VLAN Profile screen (see the previous screen).
2. Modify the settings as explained in the previous table.
3. Click **Apply** to save your settings.

➢ **To enable, disable, or delete one or more VLAN profiles:**

1. On the LAN Setup (IPv4) screen (see *Figure 27* on page 51), select the check box to the left of each VLAN profile that you want to enable, disable, or delete, or click the **Select All** table button to select all profiles. (You cannot select the default VLAN profile.)
2. Click one of the following table buttons:
   - **Enable**. Enables the VLAN or VLANs. The ! status icon changes from a gray circle to a green circle, indicating that the selected VLAN or VLANs are enabled. (By default, when a VLAN is added to the table, it is automatically enabled.)
   - **Disable**. Disables the VLAN or VLANs. The ! status icon changes from a green circle to a gray circle, indicating that the selected VLAN or VLANs are disabled.
   - **Delete**. Deletes the VLAN or VLANs.

Configure VLAN MAC Addresses and LAN Advanced Settings

By default, all configured VLAN profiles share the same single MAC address as the LAN ports. (All LAN ports share the same MAC address.) However, you can change the VLAN MAC settings to allow up to 16 VLANs to each be assigned a unique MAC address.

You can also enable or disable the broadcast of Address Resolution Protocol (ARP) packets for the default VLAN. If the broadcast of ARP packets is enabled, IP addresses can be mapped to physical addresses (that is, MAC addresses).

➢ **To configure a VLAN to have a unique MAC address:**

1. Select **Network Configuration > LAN Settings**. The LAN submenu tabs display, with the LAN Setup (IPv4) screen in view (see *Figure 27* on page 51).
2. Click the **Advanced** option arrow in the upper right of the LAN Setup (IPv4) screen. The IPv4 LAN Advanced screen displays:

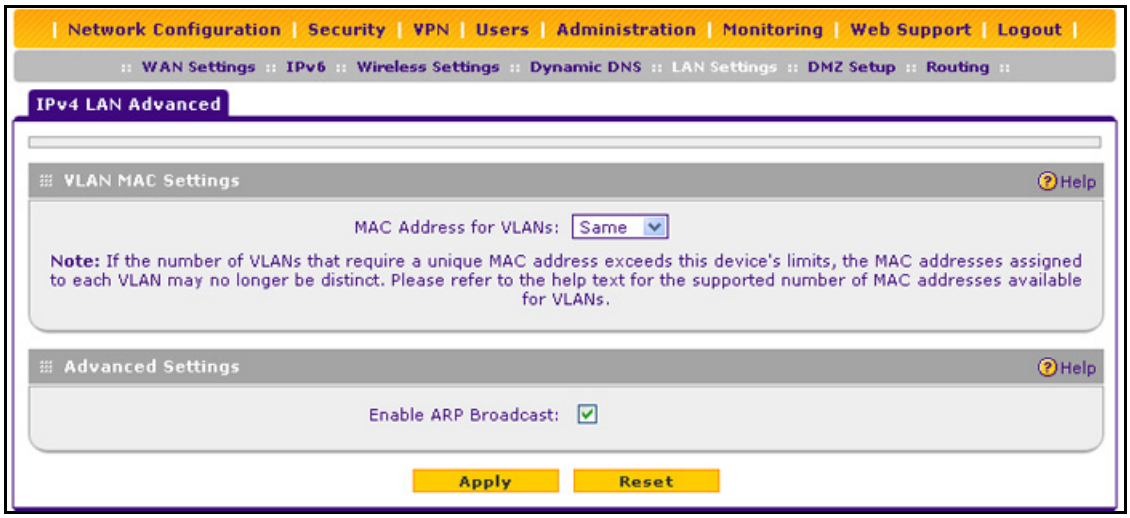

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
WAN Settings :: IPv6 :: Wireless Settings :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing
IPv4 LAN Advanced
VLAN MAC Settings
Help
MAC Address for VLANs: Same
Note: If the number of VLANs that require a unique MAC address exceeds this device's limits, the MAC addresses assigned to each VLAN may no longer be distinct. Please refer to the help text for the supported number of MAC addresses available for VLANs.
Advanced Settings
Help
Enable ARP Broadcast:
Apply
Reset

Figure 29.

3. From the MAC Address for VLANs drop-down list, select **Unique**. (The default is Same.)
4. As an option, you can disable the broadcast of ARP packets for the default VLAN by clearing the **Enable ARP Broadcast** check box. (The broadcast of ARP packets is enabled by default for the default VLAN.)
5. Click **Apply** to save your settings.

> **Note:** If you attempt to configure more than 16 VLANs while the MAC address for VLANs is set to Unique on the LAN Advanced screen, the MAC addresses that are assigned to each VLAN might no longer be distinct.

Configure IPv4 Multihome LAN IP Addresses on the Default VLAN

If you have computers using different IP networks in the LAN, (for example, 172.16.2.0 or 10.0.0.0), you can add aliases to the LAN ports and give computers on those networks access to the Internet, but you can do so only for the default VLAN. The IP address that is assigned as a secondary IP address needs to be unique and cannot be assigned to the VLAN.

It is important that you ensure that any secondary LAN addresses are different from the primary LAN, WAN, and DMZ IP addresses and subnet addresses that are already configured on the wireless VPN firewall. The following is an example of correctly configured IP addresses:

- WAN IP address. 10.0.0.1 with subnet 255.0.0.0
- DMZ IP address. 192.168.10.1 with subnet 255.255.255.0

- Primary LAN IP address. 192.168.1.1 with subnet 255.255.255.0
- Secondary LAN IP address. 192.168.20.1 with subnet 255.255.255.0

➢ **To add a secondary LAN IP address:**

1. Select **Network Configuration > LAN Settings > LAN Multi-homing (IPv4)**. The LAN Multi-homing (IPv4) screen displays. (The following figure contains one example.)

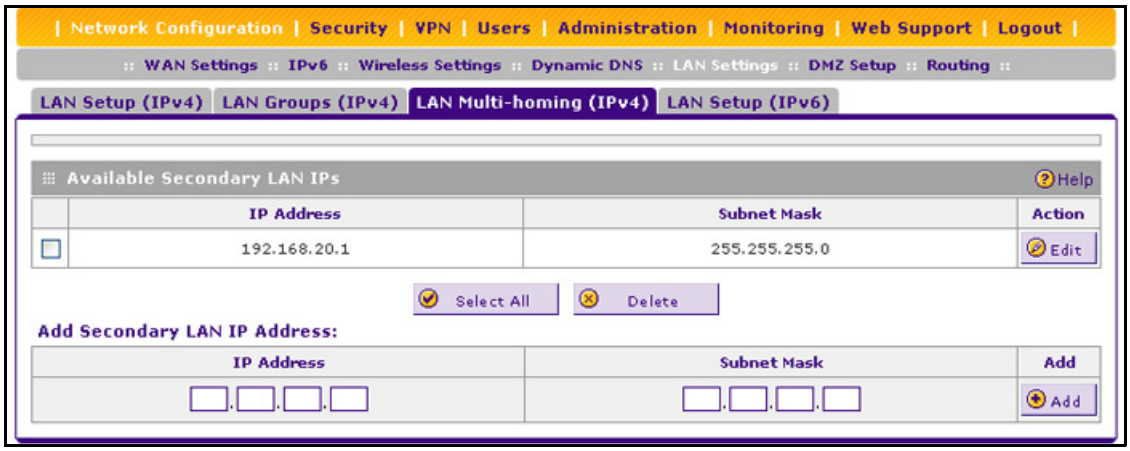

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
WAN Settings :: IPv6 :: Wireless Settings :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing
LAN Setup (IPv4) LAN Groups (IPv4) LAN Multi-homing (IPv4) LAN Setup (IPv6)
Available Secondary LAN IPs
Help
IP Address
Subnet Mask
Action
192.168.20.1
255.255.255.0
Edit
Select All
Delete
Add Secondary LAN IP Address:
IP Address
Subnet Mask
Add
Add

Figure 30.

The Available Secondary LAN IPs table displays the secondary LAN IP addresses added to the wireless VPN firewall.

2. In the Add Secondary LAN IP Address section of the screen, enter the following settings:
   - **IP Address**. Enter the secondary address that you want to assign to the LAN ports.
   - **Subnet Mask**. Enter the subnet mask for the secondary IP address.
3. Click the **Add** table button in the rightmost column to add the secondary IP address to the Available Secondary LAN IPs table.

   Repeat *step 2* and *step 3* for each secondary IP address that you want to add to the Available Secondary LAN IPs table.

Note: Secondary IP addresses cannot be configured in the DHCP server. The hosts on the secondary subnets need to be manually configured with the IP addresses, gateway IP address, and DNS server IP addresses.

➢ **To edit a secondary LAN IP address:**

1. On the LAN Multi-homing (IPv4) screen (see the previous screen), click the **Edit** button in the Action column for the secondary IP address that you want to modify. The Edit LAN Multi-homing screen displays.
2. Modify the IP address or subnet mask, or both.
3. Click **Apply** to save your settings.

➢ **To delete one or more secondary LAN IP addresses:**

1. On the LAN Multi-homing (IPv4) screen (see the previous screen), select the check box to the left of each secondary IP address that you want to delete, or click the **Select All** table button to select secondary IP addresses.
2. Click the **Delete** table button.

Manage IPv4 Groups and Hosts (IPv4 LAN Groups)

The Known PCs and Devices table on the LAN Groups (IPv4) screen (see *Figure 31* on page 60) contains a list of all known PCs and network devices that are assigned dynamic IP addresses by the wireless VPN firewall, have been discovered by other means, or were entered manually. Collectively, these entries make up the network database.

The network database is updated by these methods:

- **DHCP client requests**. When the DHCP server is enabled, it accepts and responds to DHCP client requests from PCs and other network devices. These requests also generate an entry in the network database. This is an advantage of enabling the DHCP server feature.
- **Scanning the network**. The local network is scanned using Address Resolution Protocol (ARP) requests. The ARP scan detects active devices that are not DHCP clients.

Note: In large networks, scanning the network might generate unwanted traffic.

Note: When the wireless VPN firewall receives a reply to an ARP request, it might not be able to determine the device name if the software firewall of the device blocks the name.

- **Manual entry**. You can manually enter information about a network device.

These are some advantages of the network database:

- Generally, you do not need to enter an IP address or a MAC address. Instead, you can just select the name of the desired PC or device.
- There is no need to reserve an IP address for a PC in the DHCP server. All IP address assignments made by the DHCP server are maintained until the PC or device is removed from the network database, either by expiration (inactive for a long time) or by you.
- There is no need to use a fixed IP address on a PC. Because the IP address allocated by the DHCP server never changes, you do not need to assign a fixed IP address to a PC to ensure that it always has the same IP address.

- A PC is identified by its MAC address—not its IP address. The network database uses the MAC address to identify each PC or device. Therefore, changing a PC's IP address does not affect any restrictions applied to that PC.
- Control over PCs can be assigned to groups and individuals:
  - You can assign PCs to groups (see *Manage the Network Database* on this page) and apply restrictions (outbound rules and inbound rules) to each group (see *Rules to Block or Allow Specific Kinds of Traffic* on page 108).
  - You can select groups that are allowed access to URLs that you have blocked for other groups, or the other way around, block access to URLs that you have allowed access to for groups (see *Configure Content Filtering* on page 142).
  - If necessary, you can also create firewall rules to apply to a single PC (see *Enable Source MAC Filtering* on page 147). Because the MAC address is used to identify each PC, users cannot avoid these restrictions by changing their IP address.

Manage the Network Database

You can view the network database, manually add or remove database entries, and edit database entries.

To view the network database, select **Network Configuration > LAN Settings > LAN Groups (IPv4)**. The LAN Groups (IPv4) screen displays. (The following figure shows some manually added devices in the Known PCs and Devices table as an example.)

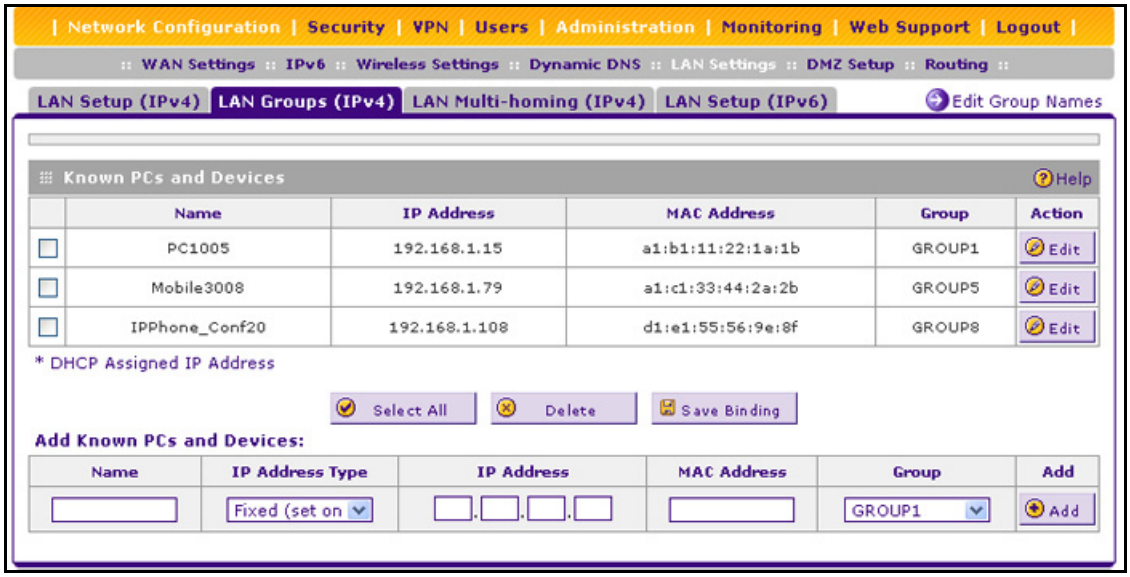

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
WAN Settings :: IPv6 :: Wireless Settings :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing
LAN Setup (IPv4) LAN Groups (IPv4) LAN Multi-homing (IPv4) LAN Setup (IPv6)
Edit Group Names
Known PCs and Devices
Help
Name IP Address MAC Address Group Action
PC1005 192.168.1.15 a1:b1:11:22:1a:1b GROUP1 Edit
Mobile3008 192.168.1.79 a1:c1:33:44:2a:2b GROUP5 Edit
IPPhone_Conf20 192.168.1.108 d1:e1:55:56:9e:8f GROUP8 Edit
* DHCP Assigned IP Address
Select All
Delete
Save Binding
Add Known PCs and Devices:
Name IP Address Type IP Address MAC Address Group Add
Fixed (set on
GROUP1
Add

Figure 31.

The Known PCs and Devices table lists the entries in the network database. For each PC or device, the following fields display:

- **Check box**. Allows you to select the PC or device in the table.
- **Name**. The name of the PC or device. For computers that do not support the NetBIOS protocol, the name is displayed as *Unknown* (you can edit the entry manually to add a meaningful name). If the PC or device was assigned an IP address by the DHCP server, then the name is appended by an asterisk.
- **IP Address**. The current IP address of the PC or device. For DHCP clients of the wireless VPN firewall, this IP address does not change. If a PC or device is assigned a static IP address, you need to update this entry manually after the IP address on the PC or device has changed.
- **MAC Address**. The MAC address of the PC or device's network interface.
- **Group**. Each PC or device can be assigned to a single LAN group. By default, a PC or device is assigned to Group 1. You can select a different LAN group from the Group drop-down list in the Add Known PCs and Devices section or on the Edit Groups and Hosts screen.
- **Action**. The Edit table button, which provides access to the Edit Groups and Hosts screen.

Add PCs or Devices to the Network Database

➢ **To add PCs or devices manually to the network database:**

1. In the Add Known PCs and Devices section of the LAN Groups screen (see the previous figure), enter the settings as explained in the following table:

Table 11. Known PCs and devices settings

Setting	Description
Name	Enter the name of the PC or device.
IP Address Type	From the drop-down list, select how the PC or device receives its IP address: • **Fixed (set on PC)**. The IP address is statically assigned on the PC or device. • **Reserved (DHCP Client)**. Directs the wireless VPN firewall's DHCP server to always assign the specified IP address to this client during the DHCP negotiation (see *Set Up Address Reservation* on page 64). **Note:** When you assign a reserved IP address to a client, the selected IP address needs to be outside the range of addresses allocated to the DHCP server pool.
IP Address	Enter the IP address that this PC or device is assigned in the IP Address field. If the IP address type is Reserved (DHCP Client), the wireless VPN firewall reserves the IP address for the associated MAC address.
MAC Address	Enter the MAC address of the PC's or device's network interface. The MAC address format is six colon-separated pairs of hexadecimal characters (0–9 and A–F), such as 01:23:45:67:89:AB.
Group	From the drop-down list, select the group to which the PC or device is assigned. (Group 1 is the default group.)

2. Click the **Add** table button to add the PC or device to the Known PCs and Devices table.
3. As an optional step: To enable DHCP address reservation for the entry that you just added to the Known PCs and Devices table, select the check box for the table entry, and click the **Save Binding** button to bind the IP address to the MAC address for DHCP assignment.

Edit PCs or Devices in the Network Database

➢ **To edit PCs or devices manually in the network database:**

1. In the Known PCs and Devices table of the LAN Groups screen (see the previous figure), click the **Edit** table button of a table entry. The Edit LAN Groups screen displays (see the following figure, which contains an example).

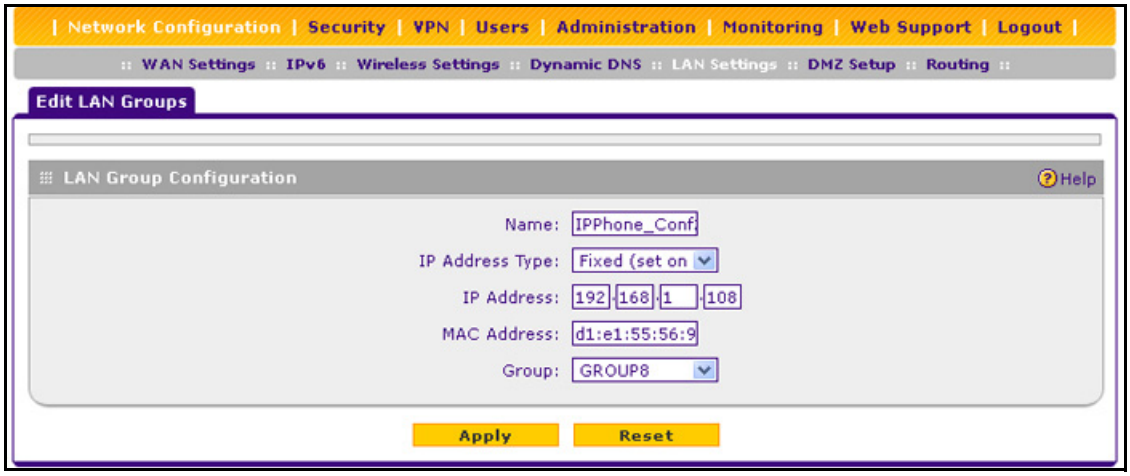

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
WAN Settings :: IPv6 :: Wireless Settings :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing
Edit LAN Groups
LAN Group Configuration
Help
Name: IPPhone_Conf
IP Address Type: Fixed (set on
IP Address: 192 168 1 108
MAC Address: d1:e1:55:56:9
Group: GROUP8
Apply
Reset

Figure 32.

2. Modify the settings as explained in *Table 11* on page 61.
3. Click **Apply** to save your settings in the Known PCs and Devices table.

Deleting PCs or Devices from the Network Database

➢ **To delete one or more PCs or devices from the network database:**

1. On the LAN Groups (IPv4) screen (see *Figure 31* on page 60), select the check box to the left of each PC or device that you want to delete, or click the **Select All** table button to select all PCs and devices.
2. Click the **Delete** table button.

Change Group Names in the Network Database

By default, the groups are named Group1 through Group8. You can change these group names to be more descriptive, such as GlobalMarketing and GlobalSales. However, note that on the Content Filtering screen (see *Configure Content Filtering* on page 142), the default group names are displayed and not the names that you specified.

➢ **To edit the names of any of the eight available groups:**

1. Select **Network Configuration > LAN Setting > LAN Groups (IPv4)**. The LAN Groups (IPv4) screen displays (see *Figure 31* on page 60, which shows some examples in the Known PCs and Devices table).
2. Click the **Edit Group Names** option arrow to the right of the LAN submenu tabs. The Network Database Group Names screen displays. (The following figure shows some examples.)

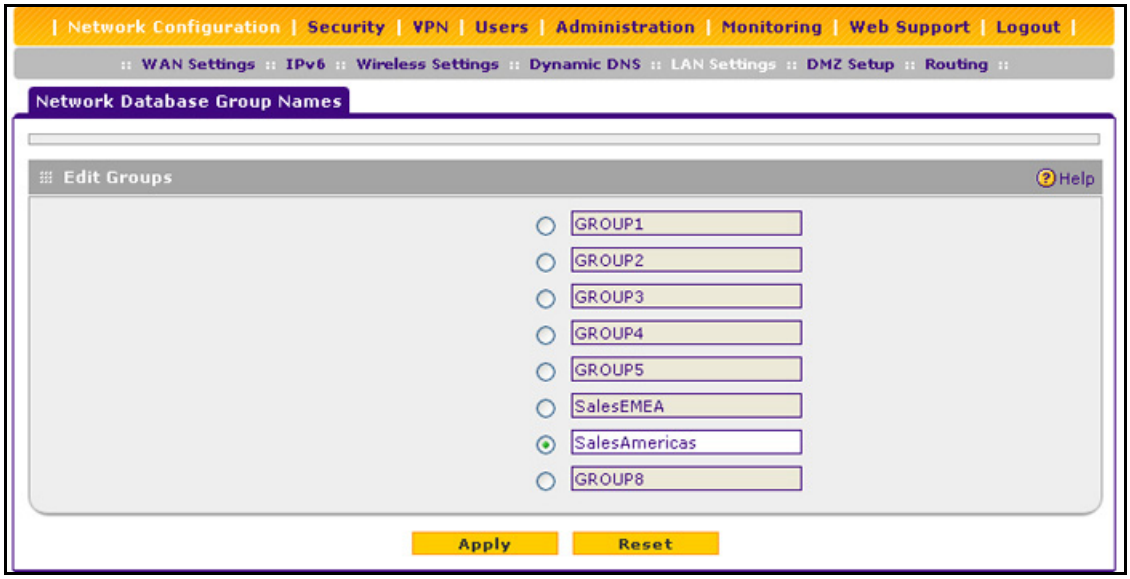


Figure 33.

3. Select the radio button next to the group name that you want to edit.
4. Type a new name in the field. The maximum number of characters is 15; spaces and double quotes (") are not allowed.
5. Repeat *step 3* and *step 4* for any other group names.
6. Click **Apply** to save your settings.

Set Up Address Reservation

When you specify a reserved IP address for a PC or device on the LAN (based on the MAC address of the device), that PC or device always receives the same IP address each time it accesses the wireless VPN firewall's DHCP server. Reserved IP addresses should be assigned to servers or access points that require permanent IP address settings. The reserved IP address that you select needs to be outside of the DHCP server pool.

To reserve an IP address, select **Reserved (DHCP Client)** from the IP Address Type drop-down list on the LAN Groups screen as described in *Add PCs or Devices to the Network Database* on page 61 or on the Edit Groups and Hosts screen as described in *Edit PCs or Devices in the Network Database* on page 62.

Note: The reserved address is not assigned until the next time the PC or device contacts the wireless VPN firewall's DHCP server. Reboot the PC or device, or access its IP configuration and force a DHCP release and renew.

Configure IPv6 LAN Settings

An IPv6 LAN typically functions with link-local unicast addresses. Each physical interface requires an IPv6 link-local address that is automatically derived from the MAC addresses of the IPv4 interface and that is used for address configuration and neighbor discovery.

Traffic with link-local addresses is never forwarded by a router, that is, the traffic remains in the LAN subnet and is processed over the default VLAN only. A link-local unicast address always starts with FE80 (hexadecimal). To forward traffic from sources with a link-local unicast address in the LAN, a DHCP server is required. For more information about link-local unicast addresses, see *ISATAP Tunnel Mechanism* on page 38.

➢ **To configure the IPv6 LAN settings:**

1. Select **Network Configuration > LAN Settings > LAN Setup (IPv6)**. The LAN Setup (IPv6) screen displays. (The following figure contains some examples.)

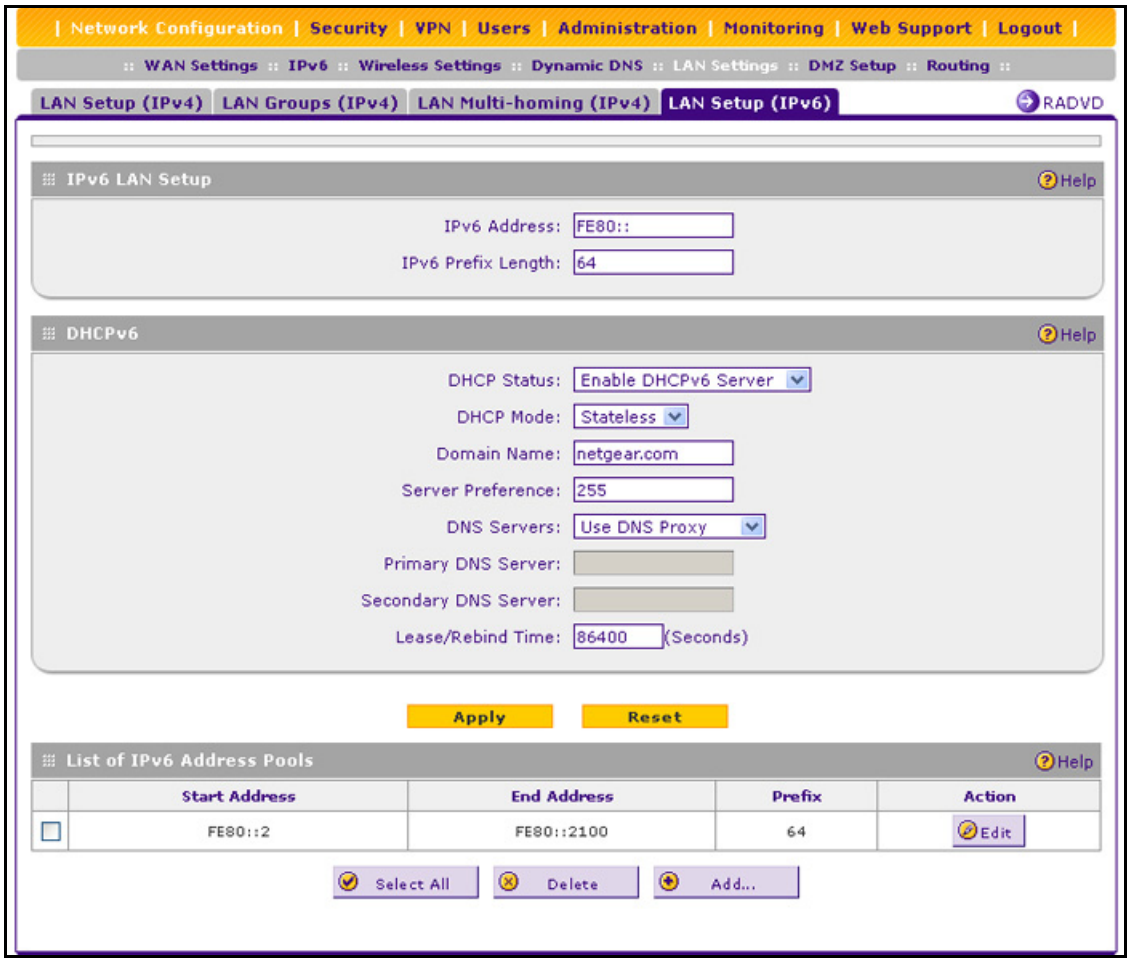


Figure 34.

2. Enter the settings as explained in the following table:

Table 12. LAN Setup (IPv6) screen settings

Setting	Description
IPv6 LAN Setup	
IPv6 Address	Enter the FE80 link-local IPv6 address.
IPv6 Prefix Length	Enter the IPv6 prefix length, for example /10 or /64.

Table 12. LAN Setup (IPv6) screen settings (continued)

Setting	Description	
DHCPv6		
DHCP Status	Specify the status of the DHCPv6 server: • **Disable DHCPv6 Server**. This is the default setting, and the DHCPv6 fields are masked out. • **Enable the DHCPv6 Server**. If you enable the server, you need to complete the DHCPv6 fields.	
	DHCP Mode	Select one of the DHCPv6 modes from the drop-down lists: • **Stateless**. The wireless VPN firewall generates its own IP address by using a combination of locally available information and router advertisements, but receives DNS server information from a DHCP server. • **Stateful**. The wireless VPN firewall obtains an interface address, configuration information such as DNS server information, and other parameters from a DHCP server. The IP address is a dynamic address. **Note:** For stateful DHCP, you need to configure IPv6 address pools (see the section following this table).
	Domain Name	Enter the domain name of the DHCP server.
	Server Preference	Enter the DHCP server preference value. The possible values are 0–255, with 0 as the default setting. This is an optional setting that specifies the server's preference value in a server advertise message. The client selects the server with the highest preference value as the preferred server.
	DNS Server	Select one of the DNS server options from the drop-down lists: • **Use DNS Proxy**. The wireless VPN firewall acts as a proxy for all DNS requests and communicates with the ISP's DNS servers that you configured on the Broadband ISP Settings (IPv6) screen (see *Manually Configure an IPv6 Internet Connection* on page 34). • **Use DNS from ISP**. The wireless VPN firewall uses the ISP's DNS servers that you configured on the Broadband ISP Settings (IPv6) screen (see *Manually Configure an IPv6 Internet Connection* on page 34). • **Use below**. When you select this option, the DNS server fields become available for you to enter IP addresses.
		Primary DNS Server: Enter the IP address of the primary DNS server.
		Secondary DNS Server: Enter the IP address of the secondary DNS server.
	Lease/Rebind Time	Enter the period after which the DHCP lease is renewed with the original DHCP server or rebound with another DHCP server to extend the existing DHCP lease. The default period is 86400 seconds (24 hours).

3. Click **Apply** to save your changes.

IPv6 Address Pools

If you configure a stateful DHCPv6 server, you need to add local DHCP IPv6 address pools so the DHCPv6 server can control the allocation of IPv6 addresses.

➢ **To add an IPv6 address pool:**

1. On the LAN Setup (IPv6) screen, under the List of IPv6 Address Pools table, click **Add**. The LAN IPv6 Config screen displays.

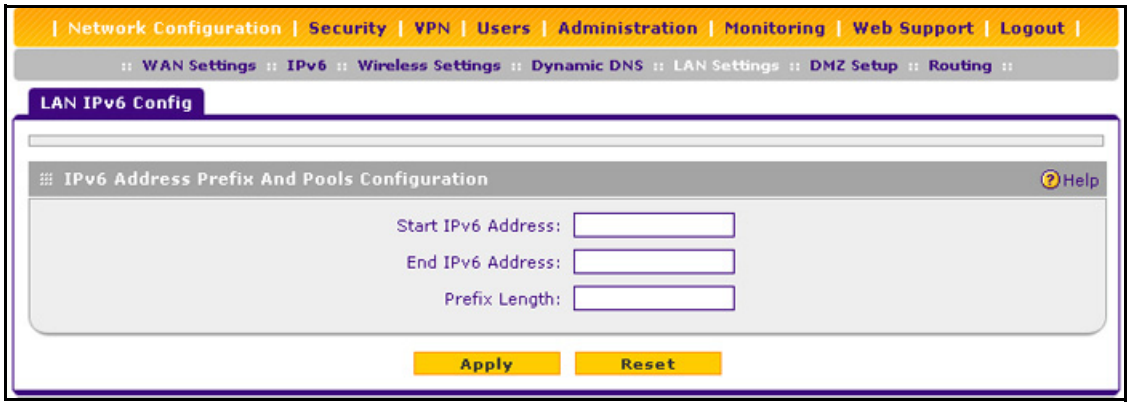

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
WAN Settings :: IPv6 :: Wireless Settings :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing
LAN IPv6 Config
IPv6 Address Prefix And Pools Configuration
Help
Start IPv6 Address:
End IPv6 Address:
Prefix Length:
Apply
Reset

Figure 35.

2. Enter the settings as explained in the following table:

Table 13. LAN IPv6 Config screen settings

Setting	Description
Start IPv6 Address	Enter the start IP address. This address specifies the first of the contiguous addresses in the IP address pool. Any new DHCPv6 client joining the LAN is assigned an IP address between this address and the end IP address.
End IPv6 Address	Enter the end IP address. This address specifies the last of the contiguous addresses in the IP address pool. Any new DHCPv6 client joining the LAN is assigned an IP address between the start IP address and this IP address.
Prefix Length	Enter the IPv6 prefix length, for example /10 or /64.

3. Click **Apply** to save your changes and add the new IPv6 address pool to the List of IPv6 Address Pools table on the LAN Setup (IPv6) screen.

➢ **To edit an IPv6 address pool:**

1. On the LAN Setup (IPv6) screen (see *Figure 34* on page 65), click the **Edit** button in the Action column for the address pool that you want to modify. The LAN IPv6 Config screen displays.
2. Modify the settings as explained in the previous table.
3. Click **Apply** to save your settings.

➢ **To delete one or more IPv6 address pools:**

1. On the LAN Setup (IPv6) screen (see *Figure 34* on page 65), select the check box to the left of each address pool that you want to delete, or click the **Select All** table button to select all address pools.
2. Click the **Delete** table button.

Configure the Router Advertisement Daemon and Advertisement Prefixes

When you configure stateful or stateless DHCPv6 (see the previous section), you also need to configure the Router Advertisement Deamon (RADVD) so that link-local advertisements of the wireless VPN firewall's IPv6 addresses and IPv6 prefixes can be automatically distributed through the Neighbor Discovery Protocol (NDP).

If you have configured stateful DHCPv6, the RADVD provides IP addresses, including the address for the gateway; the DHCP server provides DNS server information only. If you have configured stateless DHCPv6, *both* the RADVD and the DHCP server provide IP addresses, including the address for the gateway, and the DHCP server provides also DNS server information.

Hosts and routers on the LAN use NDP to determine the link-layer addresses and related information of neighbors on the LAN that can forward packets on their behalf. The wireless VPN firewall periodically distributes router advertisements (RAs) throughout the LAN to provide such information to the hosts and routers on the LAN. RAs include IPv6 addresses, types of prefixes, prefix addresses, prefix lifetimes, the maximum transmission unit (MTU), and so on. In addition to configuring the RADVD, you also need to configure the prefixes that are advertised in the RAs.

➢ **To configure the Router Advertisement Daemon:**

1. Select **Network Configuration > LAN Settings > LAN Setup (IPv6)**. The LAN Setup (IPv6) screen displays (see *Figure 34* on page 65).
2. Select the **RADVD** option arrow to the right of the LAN Setup (IPv6) tab. The RADVD screen displays. (The following figure contains some examples.)

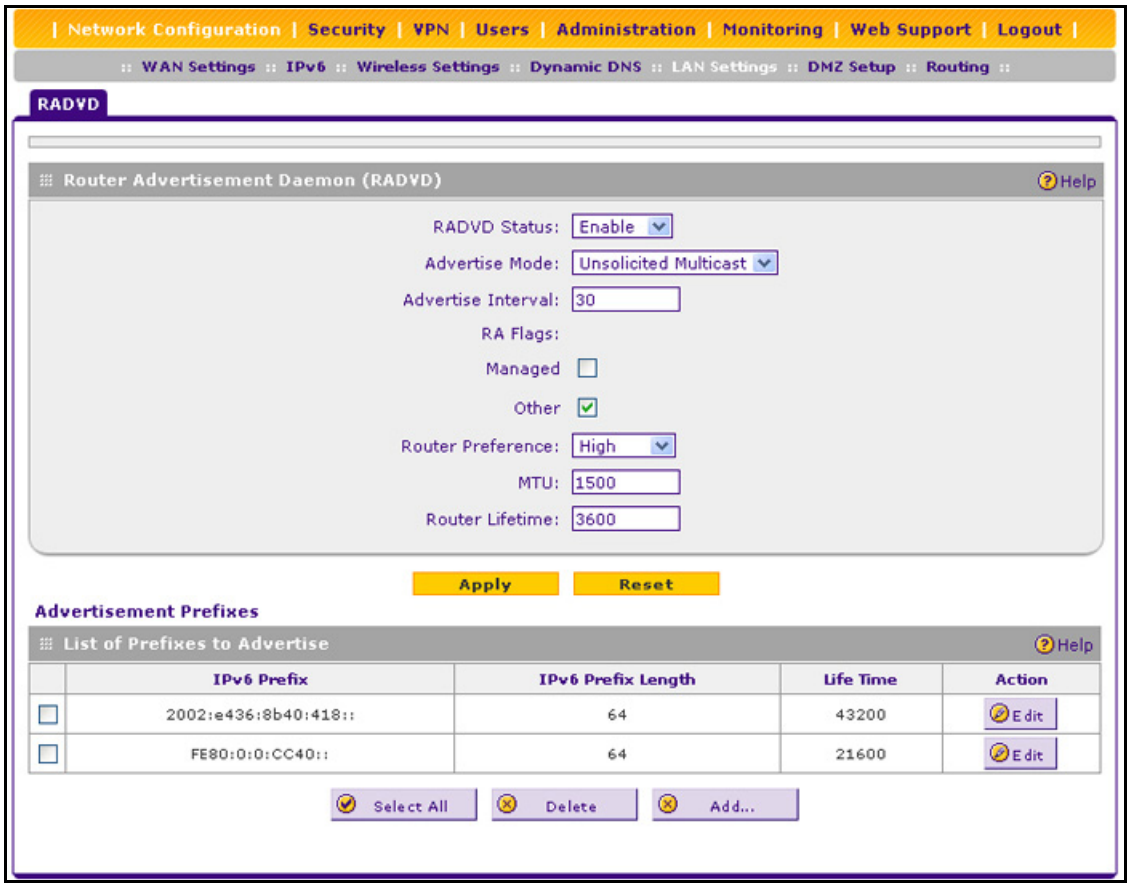


Figure 36.

3. Enter the settings as explained in the following table:

Table 14. RADVD screen settings

Setting	Description
RADVD Status	Specify the RADVD status by making a selection from the drop-down list: • **Enable**. The RADVD is enabled, and the RADVD fields become available for you to configure. • **Disable**. The RADVD is disabled, and the RADVD fields are masked out. This is the default setting.
Advertise Mode	Specify the advertisement mode by making a selection from the drop-down list: • **Unsolicited Multicast**. The wireless VPN firewall advertises unsolicited multicast packets at a rate that is specified by the advertisement interval. • **Unicast only**. The wireless VPN firewall responds to unicast packet requests only. No unsolicited packets are advertised. Select this option for nonbroadcast multiple access (NBMA) links such as ISATAP.
Advertise Interval	Enter the advertisement interval of unsolicited multicast packets in seconds. The minimum value is 10 seconds; the maximum value is 1800 seconds.

Table 14. RADVD screen settings (continued)

Setting	Description	
RA Flags	Managed	To specify that the DHCPv6 stateful protocol is used for autoconfiguration of the address, select the **Managed** check box.
	Other	To specify that other configuration information such as DNS information is available through DHCPv6, select the **Other** check box. **Note:** If the Managed check box is selected, you do not need to select the Other check box because DHCPv6 provides all configuration information.
Router Preference	Specify the wireless VPN firewall's preference in relation to other hosts and routers on the LAN by making a selection from the drop-down list: • **Low**. The wireless VPN firewall is treated as a nonpreferred router in the LAN. • **Medium**. The wireless VPN firewall is treated as a neutral router in the LAN. • **High**. The wireless VPN firewall is treated as a preferred router in the LAN.	
MTU	The maximum transmission unit (MTU) size for a packet in one transmission over a link. The default setting is 1500.	
Router Lifetime	The router lifetime specifies how long the default route that was created as a result of the router advertisement should remain valid. Enter the router lifetime in seconds. This is the period that the advertised prefixes are valid for route determination. The default period is 3600 seconds (one hour). The minimum value is 30 seconds; the maximum value is 9000 seconds.	

4. Click **Apply** to save your changes.

Advertisement Prefixes

You need to configure the prefixes that are advertised in the RAs. For a 6to4 address, you need to specify only the Site Level Aggregation Identifier (SLA ID) and the prefix lifetime. For a global, local, or ISATAP address, you need to specify the prefix, prefix length, and prefix lifetime.

➢ **To add an advertisement prefix:**

1. On the RADVD screen, under the List of Prefixes to Advertise table, click **Add**. The Add Advertisement Prefix screen displays.

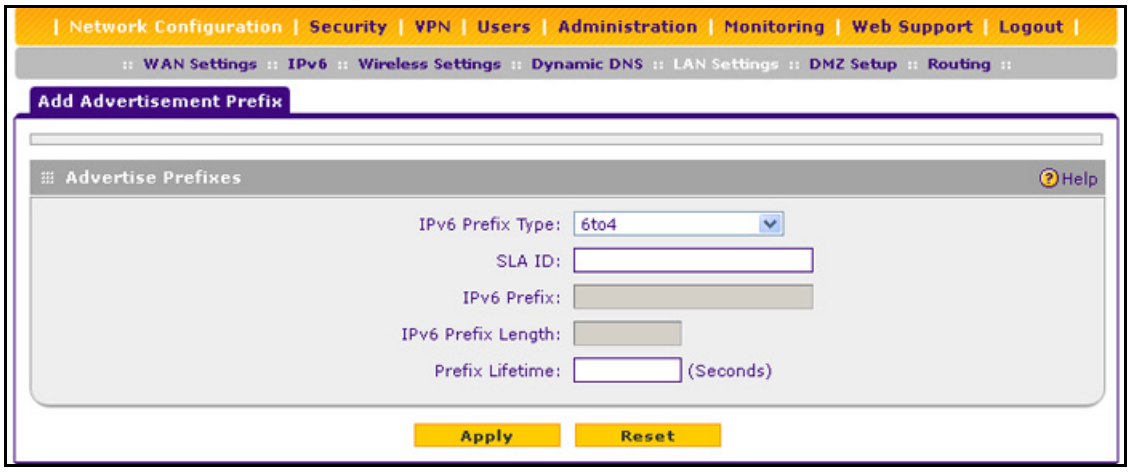

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
WAN Settings :: IPv6 :: Wireless Settings :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing
Add Advertisement Prefix
Advertise Prefixes
Help
IPv6 Prefix Type: 6to4
SLA ID:
IPv6 Prefix:
IPv6 Prefix Length:
Prefix Lifetime: (Seconds)
Apply
Reset

Figure 37.

2. Enter the settings as explained in the following table:

Table 15. Add Advertisement Prefix screen settings

Setting	Description
IPv6 Prefix Type	Specify the IPv6 prefix type making a selection from the drop-down list: • **6to4**. The prefix is for a 6to4 address. You need to complete the SLA ID field and Prefix Lifetime field. The other fields are masked out. • **Global/Local/ISATAP**. The prefix is for a global, local, or ISATAP address. This needs to be a global prefix, not the site-local or link-local prefix. You need to complete the IPv6 Prefix field, IPv6 Prefix Length field, and Prefix Lifetime field. The SLA ID field is masked out.
SLA ID	Enter the Site Level Aggregation Identifier (SLA ID) for the 6to4 address prefix that should be included in the advertisement.
IPv6 Prefix	Enter the IPv6 prefix for the wireless VPN firewall's LAN that should be included in the advertisement.
IPv6 Prefix Length	Enter the IPv6 prefix length (typically /10) that should be included in the advertisement.
Prefix Lifetime	The prefix lifetime specifies how long the IP address that was created as a result of the router advertisement should remain valid. Enter the prefix lifetime in seconds that should be included in the advertisement. The minimum period is 0 seconds; the maximum period is 65535 seconds.

3. Click **Apply** to save your changes and add the new IPv6 address pool to the List of Prefixes to Advertise table on the RADVD screen.

➢ **To edit an advertisement prefix:**

1. On the RADVD screen (see *Figure 36* on page 69), click the **Edit** button in the Action column for the advertisement prefix that you want to modify. The Add Advertisement Prefix screen displays.
2. Modify the settings as explained in the previous table.
3. Click **Apply** to save your settings.

➢ **To delete one or more advertisement prefixes:**

1. On the RADVD screen (see *Figure 36* on page 69), select the check box to the left of each advertisement prefix that you want to delete, or click the **Select All** table button to select all advertisement prefixes.
2. Click the **Delete** table button.

Configure and Enable the DMZ Port for IPv4 Traffic

The demilitarized zone (DMZ) is a network that, by default, has fewer firewall restrictions than the LAN. The DMZ can be used to host servers (such as a web server, FTP server, or email server) and provide public access to them. The rightmost LAN port on the wireless VPN firewall can be dedicated as a hardware DMZ port to safely provide services to the Internet without compromising security on your LAN.

By default, the DMZ port and both inbound and outbound DMZ traffic are disabled. Enabling the DMZ port and allowing traffic to and from the DMZ increases the traffic through the WAN ports.

Using a DMZ port is also helpful with online games and videoconferencing applications that are incompatible with NAT. The wireless VPN firewall is programmed to recognize some of these applications and to work correctly with them, but there are other applications that might not function well. In some cases, local PCs can run the application correctly if those PCs are used on the DMZ port.

Note: A separate firewall security profile is provided for the DMZ port that is also physically independent of the standard firewall security component that is used for the LAN.

The DMZ Setup screen lets you set up the DMZ port. It permits you to enable or disable the hardware DMZ port (LAN port 8; see *Front Panel* on page 14) and configure an IP address and subnet mask for the DMZ port.

➢ **To enable and configure the DMZ port:**

1. Select **Network Configuration > DMZ Setup**. The DMZ Setup screen displays:

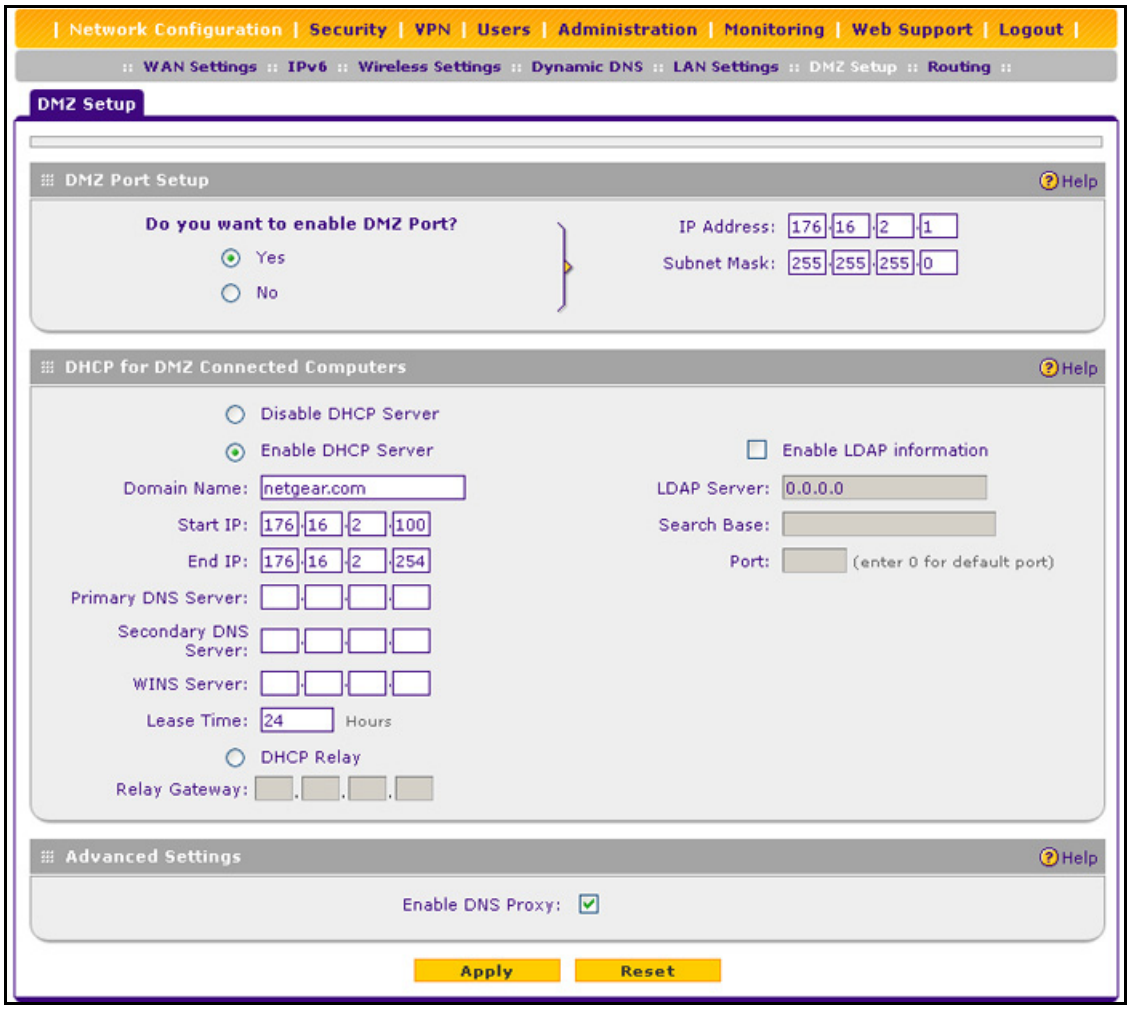

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
WAN Settings :: IPv6 :: Wireless Settings :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing
DMZ Setup
DMZ Port Setup
Help
Do you want to enable DMZ Port?
Yes
No
IP Address: 176 16 2 1
Subnet Mask: 255 255 255 0
DHCP for DMZ Connected Computers
Help
Disable DHCP Server
Enable DHCP Server
Enable LDAP information
Domain Name: netgear.com
LDAP Server: 0.0.0.0
Start IP: 176 16 2 100
Search Base:
End IP: 176 16 2 254
Port: (enter 0 for default port)
Primary DNS Server:
Secondary DNS Server:
WINS Server:
Lease Time: 24 Hours
DHCP Relay
Relay Gateway:
Advanced Settings
Help
Enable DNS Proxy:
Apply
Reset

Figure 38.

2. Enter the settings as explained in the following table:

Table 16. DMZ Setup screen settings

Setting	Description	
DMZ Port Setup		
Do you want to enable DMZ Port?	Select one of the following radio buttons: • **Yes**. Enables you to configure the DMZ port settings. Fill in the IP Address and Subnet Mask fields. • **No**. Allows you to disable the DMZ port after you have configured it.	
	IP Address	Enter the IP address of the DMZ port. Make sure that the DMZ port IP address and LAN port IP address are in different subnets (for example, an address outside the LAN address pool, such as 192.168.1.101).
	Subnet Mask	Enter the IP subnet mask of the DMZ port. The subnet mask specifies the network number portion of an IP address.

Table 16. DMZ Setup screen settings (continued)

Setting	Description	
DHCP		
Disable DHCP Server	If another device on your network is the DHCP server for the VLAN, or if you will manually configure the network settings of all of your computers, select the **Disable DHCP Server** radio button to disable the DHCP server. This is the default setting.	
Enable DHCP Server	Select the **Enable DHCP Server** radio button to enable the wireless VPN firewall to function as a Dynamic Host Configuration Protocol (DHCP) server, providing TCP/IP configuration for all computers connected to the VLAN. Enter the following settings:	
	Domain Name	This setting is optional. Enter the domain name of the wireless VPN firewall.
	Start IP Address	Enter the start IP address. This address specifies the first of the contiguous addresses in the IP address pool. Any new DHCP client joining the LAN is assigned an IP address between this address and the end IP address. The IP address 192.168.1.2 is the default start address.
	End IP Address	Enter the end IP address. This address specifies the last of the contiguous addresses in the IP address pool. Any new DHCP client joining the LAN is assigned an IP address between the start IP address and this IP address. The IP address 192.168.1.100 is the default end address. **Note:** The start and end DHCP IP addresses should be in the same network as the LAN TCP/IP address of the wireless VPN firewall (that is, the IP address in the DMZ Port Setup section as described earlier in this table).
	Primary DNS Server	This setting is optional. If an IP address is specified, the wireless VPN firewall provides this address as the primary DNS server IP address. If no address is specified, the wireless VPN firewall provides its own LAN IP address as the primary DNS server IP address.
	Secondary DNS Server	This setting is optional. If an IP address is specified, the wireless VPN firewall provides this address as the secondary DNS server IP address.
	WINS Server	This setting is optional. Enter a WINS server IP address to specify the Windows NetBIOS server, if one is present in your network.
	Lease Time	Enter a lease time. This specifies the duration for which IP addresses are leased to clients.
DHCP Relay	To use the wireless VPN firewall as a DHCP relay agent for a DHCP server somewhere else in your network, select the **DHCP Relay** radio button. Enter the following setting:	
	Relay Gateway	The IP address of the DHCP server for which the wireless VPN firewall serves as a relay.

Table 16. DMZ Setup screen settings (continued)

Setting	Description	
Enable LDAP information	To enable the DHCP server to provide Lightweight Directory Access Protocol (LDAP) server information, select the **Enable LDAP information** check box. Enter the following settings.	
	LDAP Server	The IP address or name of the LDAP server.
	Search Base	The search objects that specify the location in the directory tree from which the LDAP search begins. You can specify multiple search objects, separated by commas. The search objects include: • CN (for common name) • OU (for organizational unit) • O (for organization) • C (for country) • DC (for domain) For example, to search the Netgear.net domain for all last names of Johnson, you would enter: cn=Johnson,dc=Netgear,dc=net
	Port	The port number for the LDAP server. The default setting is 0 (zero).
DNS Proxy		
Enable DNS Proxy	This setting is optional. To enable the wireless VPN firewall to provide a LAN IP address for DNS address name resolution, select the **Enable DNS Proxy** check box. This check box is selected by default. **Note:** When the DNS Proxy option is disabled, all DHCP clients receive the DNS IP addresses of the ISP but without the DNS proxy IP address.	

3. Click **Apply** to save your settings.

Note: The DMZ LED next to LAN port 8 (see *Front Panel* on page 14) lights green to indicate that the DMZ port is enabled.

For information about how to define the DMZ WAN rules and LAN DMZ rules, see *Create DMZ WAN Rules* on page 119 and *Create LAN DMZ Rules* on page 122, respectively.

Manage Static IPv4 Routing

Static routes provide additional routing information to your wireless VPN firewall. Under normal circumstances, the wireless VPN firewall has adequate routing information after it has been configured for Internet access, and you do not need to configure additional static routes. You should configure static routes only for unusual cases such as multiple firewalls or multiple IP subnets located on your network.

Note: The wireless VPN firewall automatically sets up routes between VLANs and secondary IPv4 addresses that you have configured on the LAN Multi-homing (IPv4) screen (see *Configure IPv4 Multihome LAN IP Addresses on the Default VLAN* on page 57). Therefore, you do not need to manually add an IPv4 static route between a VLAN and a secondary IPv4 address.

Configure Static IPv4 Routes

➢ **To add an IPv4 static route to the Static Route table:**

1. Select **Network Configuration > Routing > IPv4 Static Routing**. The IPv4 Static Routing screen displays:

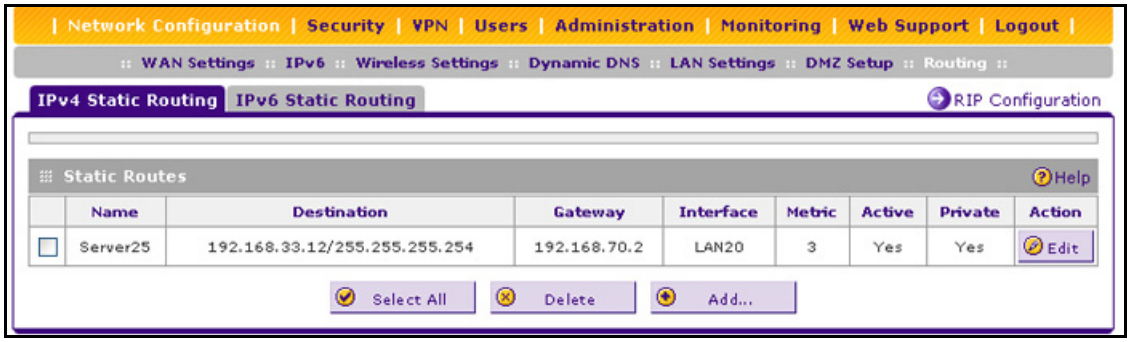


Figure 39.

2. Click the **Add** table button under the Static Routes table. The Add Static Route screen displays:

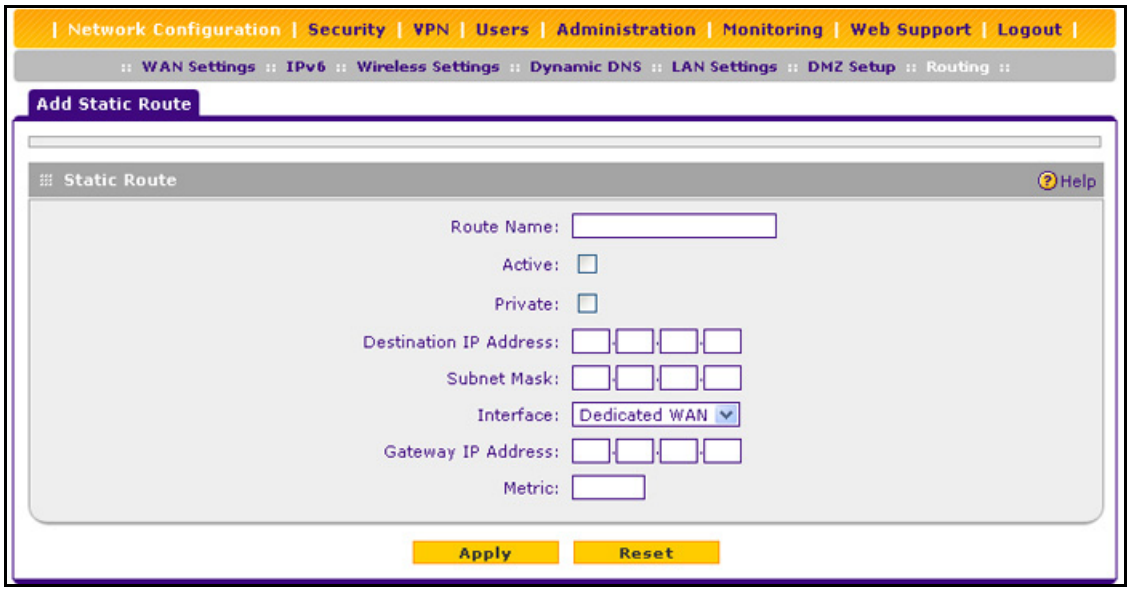


Figure 40.

3. Enter the settings as explained in the following table:

Table 17. Add Static Route screen settings

Setting	Description
Route Name	The route name for the static route (for purposes of identification and management).
Active	To make the static route effective, select the **Active** check box. **Note:** A route can be added to the table and made inactive if not needed. This allows you to use routes as needed without deleting and re-adding the entry. An inactive route is not advertised if RIP is enabled.
Private	If you want to limit access to the LAN only, select the **Private** check box. Doing so prevents the static route from being advertised in RIP.
Destination IP Address	The destination IP address of the host or network to which the route leads.
Subnet Mask	The IP subnet mask of the host or network to which the route leads. If the destination is a single host, enter **255.255.255.255**.
Interface	From the drop-down list, select the physical or virtual network interface (WAN, LAN, or DMZ interface) through which the route is accessible.
Gateway IP Address	The gateway IP address through which the destination host or network can be reached.
Metric	The priority of the route. Select a value between 2 and 15. If multiple routes to the same destination exist, the route with the lowest metric is used.

4. Click **Apply** to save your settings. The new static route is added to the Static Routes table.

➢ **To edit an IPv4 static route:**

1. On the IPv4 Static Routing screen (see *Figure 39* on page 76), click the **Edit** button in the Action column for the route that you want to modify. The Edit Static Route screen displays. This screen is identical to the Add Static Route screen (see the previous screen).
2. Modify the settings as explained in the previous table.
3. Click **Apply** to save your settings.

➢ **To delete one or more routes:**

1. On the IPv4 Static Routing screen (see *Figure 39* on page 76), select the check box to the left of each route that you want to delete, or click the **Select All** table button to select all routes.
2. Click the **Delete** table button.

Configure the Routing Information Protocol

Routing Information Protocol (RIP), RFC 2453, is an Interior Gateway Protocol (IGP) that is commonly used in internal IPv4 networks (LANs). RIP enables a router to exchange its routing information automatically with other routers, to dynamically adjust its routing tables, and to adapt to changes in the network. RIP is disabled by default. RIP does not apply to IPv6.

➢ **To enable and configure RIP:**

1. Select **Network Configuration > Routing > IPv4 Static Routing**.
2. Click the **RIP Configuration** option arrow to the right of the Routing submenu tab. The RIP Configuration screen displays:

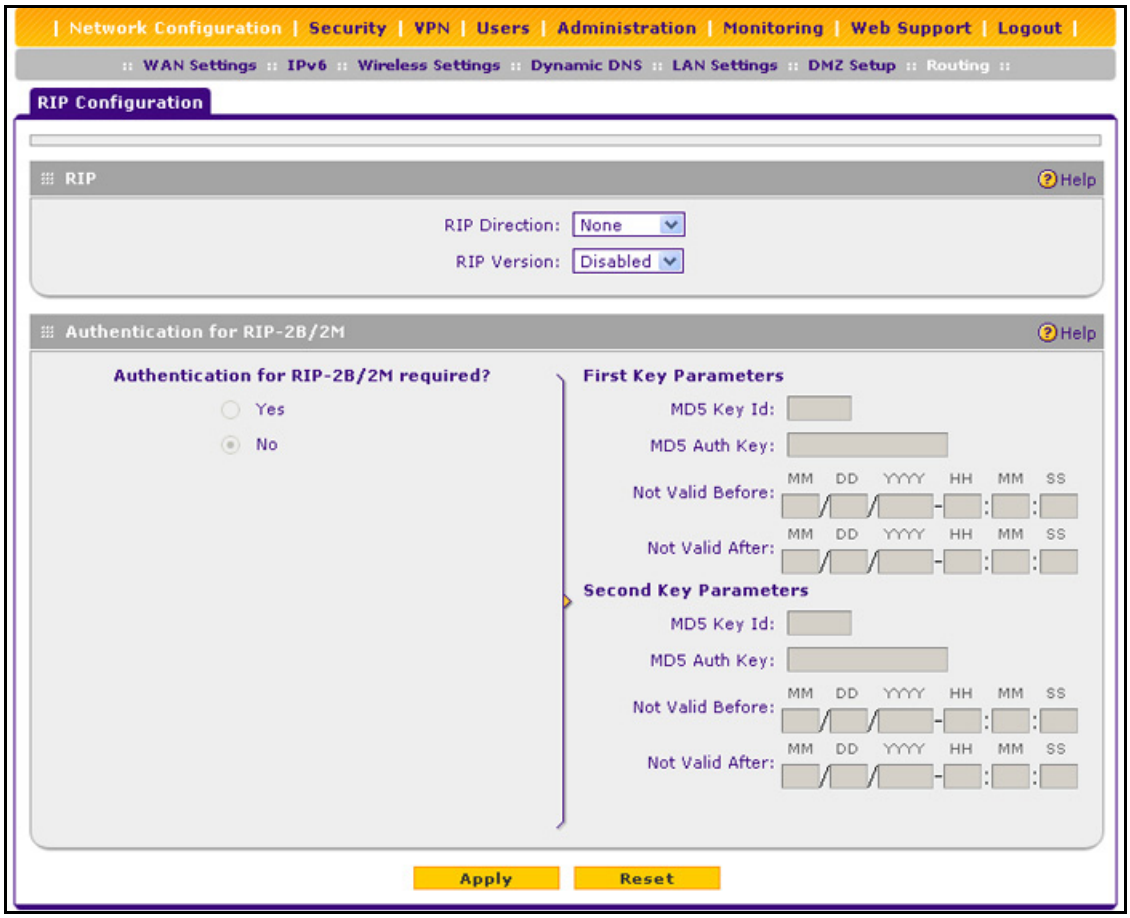

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
WAN Settings :: IPv6 :: Wireless Settings :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing
RIP Configuration
RIP
Help
RIP Direction: None
RIP Version: Disabled
Authentication for RIP-2B/2M
Help
Authentication for RIP-2B/2M required?
Yes
No
First Key Parameters
MD5 Key Id:
MD5 Auth Key:
Not Valid Before: MM DD YYYY HH MM SS
Not Valid After: MM DD YYYY HH MM SS
Second Key Parameters
MD5 Key Id:
MD5 Auth Key:
Not Valid Before: MM DD YYYY HH MM SS
Not Valid After: MM DD YYYY HH MM SS
Apply
Reset

Figure 41.

3. Enter the settings as explained in the following table:

Table 18. RIP Configuration screen settings

Setting	Description
RIP	
RIP Direction	From the RIP Direction drop-down list, select the direction in which the wireless VPN firewall sends and receives RIP packets: • **None**. The wireless VPN firewall neither advertises its route table, nor accepts any RIP packets from other routers. This effectively disables RIP, and is the default setting. • **In Only**. The wireless VPN firewall accepts RIP information from other routers but does not advertise its routing table. • **Out Only**. The wireless VPN firewall advertises its routing table but does not accept RIP information from other routers. • **Both**. The wireless VPN firewall advertises its routing table and also processes RIP information received from other routers.

Table 18. RIP Configuration screen settings (continued)

Setting	Description	
RIP Version	By default, the RIP version is set to Disabled. From the RIP Version drop-down list, select the version: • **RIP-1**. Classful routing that does not include subnet information. This is the most commonly supported version. • **RIP-2**. Routing that supports subnet information. Both RIP-2B and RIP-2M send the routing data in RIP-2 format: - **RIP-2B**. Sends the routing data in RIP-2 format and uses subnet broadcasting. - **RIP-2M**. Sends the routing data in RIP-2 format and uses multicasting.	
Authentication for RIP-2B/2M		
Authentication for RIP-2B/2M required?	Authentication for RP-2B or RIP-2M is disabled by default, that is, the No radio button is selected. To enable authentication for RP-2B or RIP-2M, select the **Yes** radio button, and enter the settings for the following fields.	
	First Key Parameters	
	MD5 Key Id	The identifier for the key that is used for authentication.
	MD5 Auth Key	The password that is used for MD5 authentication.
	Not Valid Before	The beginning of the lifetime of the MD5 key. Enter the month, date, year, hour, minute, and second. Before this date and time, the MD5 key is not valid.
	Not Valid After	The end of the lifetime of the MD5 key. Enter the month, date, year, hour, minute, and second. After this date and time, the MD5 key is no longer valid.
	Second Key Parameters	
	MD5 Key Id	The identifier for the key that is used for authentication.
	MD5 Auth Key	The password that is used for MD5 authentication.
	Not Valid Before	The beginning of the lifetime of the MD5 key. Enter the month, date, year, hour, minute, and second. Before this date and time, the MD5 key is not valid.
	Not Valid After	The end of the lifetime of the MD5 key. Enter the month, date, year, hour, minute, and second. After this date and time, the MD5 key is no longer valid.

4. Click **Apply** to save your settings.

IPv4 Static Route Example

In this example, we assume the following:

- The wireless VPN firewall's primary Internet access is through a cable modem to an ISP.
- The wireless VPN firewall is on a local LAN with IP address 192.168.1.100.
- The wireless VPN firewall connects to a remote network where you need to access a device.
- The LAN IP address of the remote network is 134.177.0.0.

When you first configured the wireless VPN firewall, two implicit static routes were created:

- A default static route was created with your ISP as the gateway.
- A second static route was created to the local LAN for all 192.168.1.x addresses.

With this configuration, if you attempt to access a device on the 134.177.0.0 remote network, the wireless VPN firewall forwards your request to the ISP. In turn, the ISP forwards your request to the remote network, where the request is likely to be denied by the remote network's firewall.

In this case, you need to define a static route, informing the wireless VPN firewall that the 134.177.0.0 IP address should be accessed through the local LAN IP address (192.168.1.100).

The static route on the wireless VPN firewall needs to be defined as follows:

- The destination IP address and IP subnet mask need to specify that the static route applies to all 134.177.x.x IP addresses.
- The gateway IP address needs to specify that all traffic for the 134.177.x.x IP addresses should be forwarded to the local LAN IP address (192.168.1.100).
- A metric value of 1 should work since the wireless VPN firewall is on the local LAN.
- The static route can be made private only as a precautionary security measure in case RIP is activated.

Manage Static IPv6 Routing

IPv6 does not use RIP to exchange routing information, and dynamic changes to IPv6 routes are not possible. To enable routers to exchange information over a static IPv6 route, you need to manually configure the static route information on each router.

➢ **To add an IPv6 static route to the Static Route table:**

1. Select **Network Configuration > Routing > IPv6 Static Routing**. The IPv6 Static Routing screen displays:

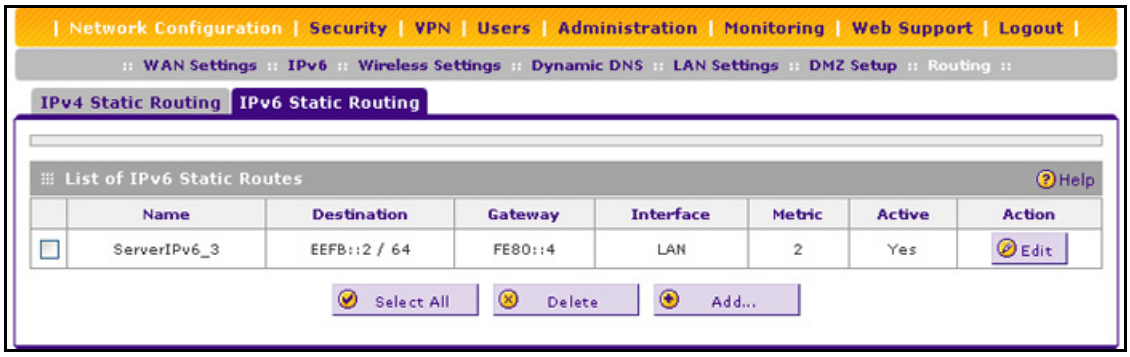


Figure 42.

2. Click the **Add** table button under the Static Routes table. The Add Static Route screen displays (the tab shows IPv6 Static Routing).

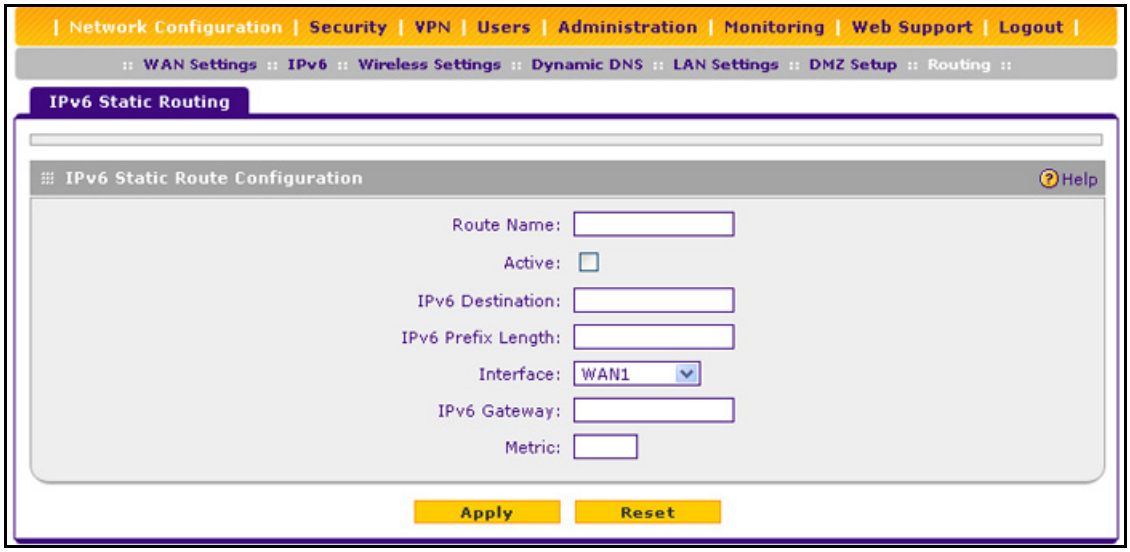


Figure 43.

3. Enter the settings as explained in the following table:

Table 19. Add Static Route screen settings

Setting	Description
Route Name	The route name for the static route (for purposes of identification and management).
Active	To make the static route effective, select the **Active** check box. **Note:** A route can be added to the table and made inactive if not needed. This allows you to use routes as needed without deleting and re-adding the entry.
IPv6 Destination	The destination IPv6 address of the host or network to which the route leads.
IPv6 Prefix Length	The destination IPv6 prefix length of the host or network to which the route leads.

Table 19. Add Static Route screen settings (continued)

Setting	Description
Interface	From the drop-down list, select the physical or virtual network interface (WAN1, sit0 Tunnel, or LAN) through which the route is accessible.
IPv6 Gateway	The gateway IPv6 address through which the destination host or network can be reached.
Metric	The priority of the route. Select a value between 2 and 15. If multiple routes to the same destination exist, the route with the lowest metric is used.

4. Click **Apply** to save your settings. The new static route is added to the List of IPv6 Static Routes table.

➢ **To edit an IPv6 static route:**

1. On the IPv6 Static Routing screen (see *Figure 42* on page 82), click the **Edit** button in the Action column for the route that you want to modify. The Edit Static Route screen displays. This screen is identical to the Add Static Route screen.
2. Modify the settings as explained in the previous table.
3. Click **Apply** to save your settings.

➢ **To delete one or more routes:**

1. On the IPv6 Static Routing screen (see *Figure 42* on page 82), select the check box to the left of each route that you want to delete, or click the **Select All** table button to select all routes.
2. Click the **Delete** table button.

Wireless Configuration and Security

4

This chapter describes how to configure the wireless features of your ProSafe Wireless-N 8-Port Gigabit VPN Firewall FVS318N. This chapter includes the following sections:

- *Overview of the Wireless Features*
- *Configure the Basic Radio Settings*
- *Wireless Data Security Options*
- *Wireless Security Profiles*
- *Configure Virtual Access Points*
- *Configure Wi-Fi Protected Setup*
- *Configure Advanced Radio Settings*
- *Test Basic Wireless Connectivity*

Before you set up the wireless features that are described in this chapter, connect the wireless VPN firewall and get the Internet connection working. The wireless VPN firewall should work with an Ethernet WAN connection. In planning your wireless network, consider the level of security required.

WARNING!

If you are configuring the wireless settings from a wireless computer and you change the wireless VPN firewall's SSID, channel, or wireless security settings, you will lose your wireless connection when you click Apply. You then need to change the wireless settings of your computer to match the wireless VPN firewall's new settings.

Overview of the Wireless Features

The wireless VPN firewall integrates a single 2.4 GHz radio and physical access point that provides 2.4 GHz 802.11b/g/n connectivity between wired Ethernet networks and radio-equipped wireless notebook systems, desktop systems, print servers, and other devices. You can configure up to four virtual access points (VAPs), each with a unique

security profile and SSID, allowing you to tailor access and security to a variety of wireless clients.

The wireless VPN firewall provides wireless connectivity to multiple wireless network devices within a fixed range or area of coverage—interacting with a wireless network interface card (NIC) through an antenna. Typically, an individual in-building wireless access point provides a maximum connectivity area of about a 500-foot radius. The wireless VPN firewall can support a small group of wireless users—typically 10 to 32 users.

Configure the wireless features according to the order of the following sections:

1. *Configure the Basic Radio Settings*
2. *Configure and Enable Wireless Security Profiles*
3. *Configure Virtual Access Points*
4. (Optional) *Configure Wi-Fi Protected Setup*
5. (Optional) *Configure Advanced Radio Settings*

Wireless Equipment Placement and Range Guidelines

The range of your wireless connection can vary significantly based on the location of the wireless VPN firewall. The latency, data throughput performance, and notebook power consumption of wireless adapters also vary depending on your configuration choices.

Note: Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the wireless VPN firewall. For complete performance specifications, see the Data Sheet on the NETGEAR website.

For best results, place your wireless VPN firewall according to the following general guidelines:

- Near the center of the area in which your wireless devices will operate.
- In an elevated location such as a high shelf where the wirelessly connected devices have line-of-sight access (even if through walls).
- Away from sources of interference, such as PCs, microwaves ovens, and 2.4-GHz cordless phones.
- Away from large metal surfaces or water.
- Placing the antennas in a vertical position provides the best side-to-side coverage. Placing the antennas in a horizontal position provides the best up-and-down coverage.
- If you are using multiple wireless VPN firewalls, it is better if adjacent wireless VPN firewalls use different radio frequency channels to reduce interference. The recommended channel space between adjacent wireless VPN firewalls is five channels (for example, use channels 1 and 6, or 6 and 11, or 1 and 11).

- The time it takes to establish a wireless connection can vary depending on both your security settings and placement. WEP connections can take slightly longer to establish. Also, WEP encryption can consume more battery power on a notebook computer.

Configure the Basic Radio Settings

The radio settings apply to all virtual access points on the wireless VPN firewall. The default wireless mode is 802.11ng. You can change the wireless mode, country, and many other radio settings on the Radio Settings screen (described in this section) and on the Advanced Wireless screen (see *Configure Advanced Radio Settings* on page 104). The default radio settings should work well for most configurations.

Note: To configure radio settings, you first need to disable the access points.

➢ **To configure the basic radio settings:**

1. Select **Network Configuration > Wireless Settings > Radio Settings**. The Radio Settings screen displays:

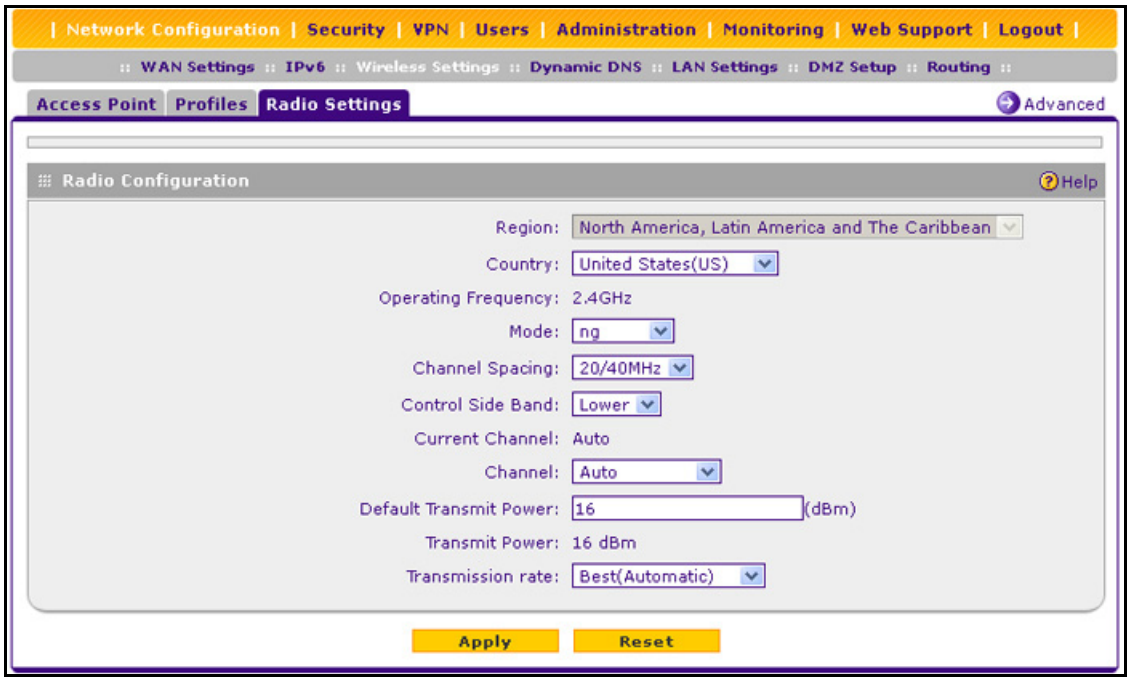

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
WAN Settings :: IPv6 :: Wireless Settings :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing
Access Point
Profiles
Radio Settings
Advanced
Radio Configuration
Help
Region: North America, Latin America and The Caribbean
Country: United States(US)
Operating Frequency: 2.4GHz
Mode: ng
Channel Spacing: 20/40MHz
Control Side Band: Lower
Current Channel: Auto
Channel: Auto
Default Transmit Power: 16 (dBm)
Transmit Power: 16 dBm
Transmission rate: Best(Automatic)
Apply
Reset

Figure 44.

2. Specify the remaining wireless settings as explained the following table:

Table 20. Radio Settings screen settings

Field	Descriptions
Region	This is a preconfigured field that you cannot change.
Country	Specify a country by making a selection from the drop-down list.
Operating Frequency	This is a nonconfigurable field. The radio's operating frequency is fixed at 2.4 GHz.
Mode	Specify the wireless mode in the 2.4-GHz band by making a selection from the drop-down list: • **g and b**. In addition to 802.11b- and 802.11g-compliant devices, 802.11n-compliant devices can connect to the wireless access point because they are backward compatible. • **g only**. 802.11g- and 802.11n-compliant devices can connect to the wireless access point, but 802.11n-compliant devices function below their capacity in 802.11g mode. 802.11b-compliant devices cannot connect. • **ng**. This is the default setting. 802.11g- and 802.11n-compliant devices can connect to the wireless access point. 802.11b-compliant devices cannot connect. • **n only**. Only 802.11n-compliant devices can connect to the wireless access point.
Channel Spacing	For the ng and n only modes, specify the channel spacing by making a selection from the drop-down list: • **20/40MHz**. Select this option to improve the performance. Some legacy devices (that is, devices that function only in b or g mode) can operate only in 20 MHz. • **20MHz**. Select this option if your network includes legacy devices. This is the default setting. **Note:** The channel spacing is fixed at 20 MHz for the g and b and g only modes.
Control Side Band **Note:** ng and n only modes only	For the ng and n only modes, when you have selected a channel spacing of 20/40MHz, you also need to select the control side band from the drop-down list. The extension channel that is specified by the control side band is four channels above or below the main channel. • **Lower**. The radio can use a lower channel (in the 1–9 range) as its extension channel. Use this setting when your main channel is in the 5–11 range. Lower is the default setting. • **Upper**. The radio can use a higher channel (in the 5–13 range) as its extension channel. Use this setting when your main channel is in the 1–7 range. **Note:** This field is not applicable when the channel spacing is set to 20 MHz.
Current Channel	This is a nonconfigurable field that shows the current channel if you have selected Auto from the Channel drop-down list.

Table 20. Radio Settings screen settings (continued)

Field	Descriptions
Channel	Specify the channel you wish to use on your wireless LAN by making a selection from the drop-down list. The wireless channels and frequencies depend on the country and wireless mode. The default setting is Auto. **Note:** It should not be necessary to change the wireless channel unless you notice interference in the network (indicated by lost connections or slow data transfers). If this happens, you might want to experiment with different channels to see which is the best. For more information, see *Operating Frequency (Channel) Guidelines* following this table. **Note:** For more information about available channels and frequencies, see *Physical and Technical Specifications* on page 333.
Default Transmit Power	Enter the default transmit power, which can range from 0 to 31. If the country regulation does not allow the transmit power that you entered, the power will be automatically adjusted to the legally allowed power, which is then displayed in the Transmit Power field.
Transmit Power	This is a nonconfigurable field that shows the actual transmit power.
Transmission rate	Specify the transmission data rate by making a selection from the drop-down list. The default setting is Best (Automatic). **Note:** For information about the available MCS indexes and transmission data rates, see *Physical and Technical Specifications* on page 333.

WARNING!

When you have changed the country settings, the wireless VPN firewall will reboot when you click Apply.

3. Click **Apply** to save your settings.

Operating Frequency (Channel) Guidelines

You should not need to change the operating frequency (channel) unless you notice interference problems, or are setting up the wireless VPN firewall near another wireless access point. Observe the following guidelines:

- Wireless access points use a fixed channel. You can select a channel that provides the least interference and best performance. In the United States and Canada, 11 channels are available.
- If you are using multiple wireless access points, it is better if adjacent wireless access points use different channels to reduce interference. The recommended channel spacing between adjacent wireless access points is 5 channels (for example, use channels 1 and 6, or 6 and 11).

- In infrastructure mode, wireless devices normally scan all channels, looking for a wireless access point. If more than one wireless access point can be used, the one with the strongest signal is used. This can happen only when the wireless access points use the same SSID. The FVS318N wireless VPN firewall functions in infrastructure mode by default.

Wireless Data Security Options

Indoors, computers can connect over 802.11n wireless networks at a maximum range of 300 feet. Typically, a wireless VPN firewall inside a building works best with devices within a 100 foot radius. Such distances can allow for others outside your immediate area to access your network.

Unlike wired network data, your wireless data transmissions can extend beyond your walls and can be received by anyone with a compatible adapter. For this reason, use the security features of your wireless equipment. The wireless VPN firewall provides highly effective security features that are covered in detail in this chapter. Deploy the security features appropriate to your needs.

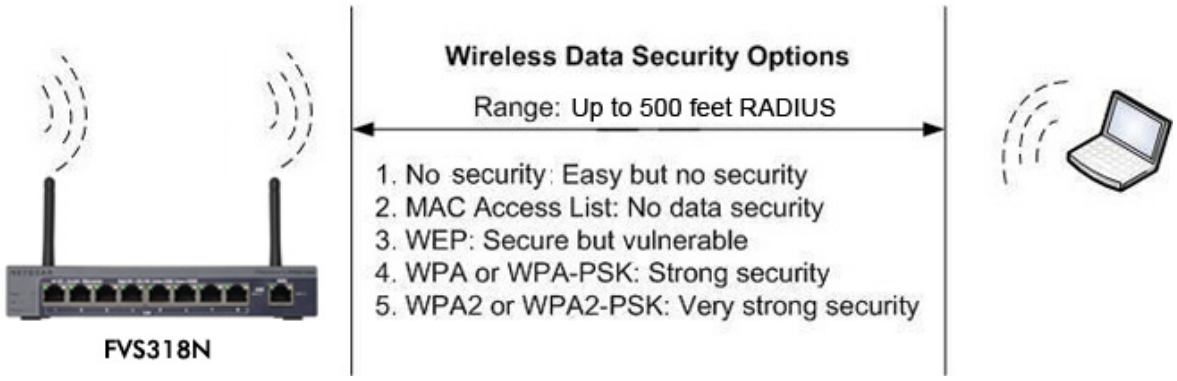

Wireless Data Security Options
Range: Up to 500 feet RADIUS
1. No security: Easy but no security
2. MAC Access List: No data security
3. WEP: Secure but vulnerable
4. WPA or WPA-PSK: Strong security
5. WPA2 or WPA2-PSK: Very strong security
FVS318N

Figure 45.

There are several ways you can enhance the security of your wireless network:

- **Restrict access based by MAC address**. You can allow only trusted PCs to connect so that unknown PCs cannot wirelessly connect to the wireless VPN firewall. Restricting access by MAC address adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed. For information about how to restrict access by MAC address, see *Restrict Wireless Access by MAC Address* on page 101.
- **Turn off the broadcast of the wireless network name (SSID)**. If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies the wireless network discovery feature of some products, such as Windows XP, but the data is still exposed. For information about how to turn of broadcast of the SSID, see *Configure and Enable Wireless Security Profiles* on page 93.
- **WEP**. Wired Equivalent Privacy (WEP) data encryption provides data security. WEP shared key authentication and WEP data encryption block all but the most determined

eavesdropper. This data encryption mode has been superseded by WPA-PSK and WPA2-PSK.

For information about how to configure WEP, see *Configure and Enable Wireless Security Profiles* on page 93.

- **WPA**. Wi-Fi Protected Access (WPA) data encryption provides strong data security with Temporal Key Integrity Protocol (TKIP) or a combination of TKIP and Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) encryption. The very strong authentication along with dynamic per frame rekeying of WPA make it virtually impossible to compromise. The wireless VPN firewall supports WPA with a pre-shared key (PSK), RADIUS, or a combination of PSK and RADIUS.

  For more information about how to configure WPA, see *Configure and Enable Wireless Security Profiles* on page 93.

- **WPA2**. Wi-Fi Protected Access version 2 (WPA2) data encryption provides strong data security with CCMP encryption or a combination of TKIP and CCMP encryption. WPA2 provides the most reliable security. Use WPA2 only if all clients in your network support WPA2. The wireless VPN firewall supports WPA2 with PSK, RADIUS, or a combination of PSK and RADIUS.

  For more information about how to configure WPA2, see *Configure and Enable Wireless Security Profiles* on page 93.

- **WPA+WPA2 mixed mode**. This mode supports data encryption with a combination of TKIP and CCMP for both WPA and WPA2 clients. The very strong authentication along with dynamic per frame rekeying of WPA2 make it virtually impossible to compromise. The wireless VPN firewall supports WPA+WPA2 with PSK, RADIUS, or a combination of PSK and RADIUS.

  For more information about how to configure WPA+WPA2 mixed mode, see *Configure and Enable Wireless Security Profiles* on page 93.

Note: TKIP provides only legacy (slower) rates of operation. NETGEAR recommends WPA2 with CCMP to make use of 802.11n rates and speed.

Wireless Security Profiles

Security profiles let you configure unique security settings for each SSID on the wireless VPN firewall. The wireless VPN firewall supports up to four security profiles (BSSIDs) that you can configure from the Profiles screen (see *Configure and Enable Wireless Security Profiles* on page 93).

To set up a security profile, specify a name for the profile and the SSID, type of security with authentication and data encryption, and whether or not the SSID is broadcast.

- **Network authentication**
  The wireless VPN firewall is set by default as an open system with no authentication. When you configure network authentication, bear in mind that older wireless adapters might not support WPA or WPA2. Windows XP, Windows 2000 with Service Pack 3, and Windows Vista do include the client software that supports WPA. However, client software is required on the client. Consult the product documentation for your wireless adapter and WPA or WPA2 client software for instructions on configuring WPA2 settings.

  For information about the types of network authentication that the wireless VPN firewall supports, see *Configure and Enable Wireless Security Profiles* on page 93.

- **Data encryption**
  Select the data encryption that you want to use. The available options depend on the network authentication setting described earlier (otherwise, the default is None). The data encryption settings are explained in *Configure and Enable Wireless Security Profiles* on page 93.

Some concepts and guidelines regarding the SSID are:

- A basic service set (BSS) is a group of wireless devices and a single wireless access point, all using the same security profile or service set identifier (BSSID). The actual identifier in the BSSID is the MAC address of the wireless radio. (A wireless radio can have multiple MAC addresses, one for each security profile.)
- An extended service set (ESS) is a group of wireless devices, all using the same identifier (ESSID).
- Different devices within an ESS can use different channels. To reduce interference, adjacent devices should use different channels.
- Roaming is the ability of wireless devices to connect wirelessly when they physically move from one BSS to another one within the same ESS. The wireless device automatically changes to the wireless access point with the least interference or best performance.

Before You Change the SSID, WEP, and WPA Settings

For a new wireless network, print or copy the following form and fill in the settings. For an existing wireless network, the network administrator can provide this information. Be sure to set the Country/Region correctly as the first step.

Store this information in a safe place:

- **SSID**
  The service set identifier (SSID) identifies the wireless local area network. You can customize it by using up to 32 alphanumeric characters. Write your SSID on the line.

  SSID: _____

  The SSID in the wireless access point is the SSID you configure on the wireless adapter card. All wireless nodes in the same network need to be configured with the same SSID.

- **WEP key size, key format, authentication type, and passphrase**
  Choose the key size by circling one: 64 or 128 bits.
  Choose the key format by circling one: ASCII or HEX.
  Choose the authentication type by circling one: Open or Shared.

  Passphrase: _____

  Note: If you select shared key, the other devices in the network will not connect unless they are set to shared key and have the same keys in the same positions as those in the wireless VPN firewall.

- **WPA-PSK (Pre-Shared Key) and WPA2-PSK**
  Record the WPA-PSK passphrase:

  WPA-PSK passphrase: _____

  Record the WPA2-PSK passphrase:

  WPA2-PSK passphrase: _____

- **WPA RADIUS settings**
  For WPA, record the following settings for the primary and secondary RADIUS servers:

  Server name/IP address: Primary _____ Secondary _____

  Port: _____

  Shared secret: _____

- **WPA2 RADIUS settings**
  For WPA2, record the following settings for the primary and secondary RADIUS servers:

  Server name/IP address: Primary _____ Secondary _____

  Port: _____

  Shared secret: _____

Configure and Enable Wireless Security Profiles

➢ **To add a wireless security profile:**

1. Select **Network Configuration > Wireless Settings > Profiles**. The Profiles screen displays. (The following figure shows some examples.)

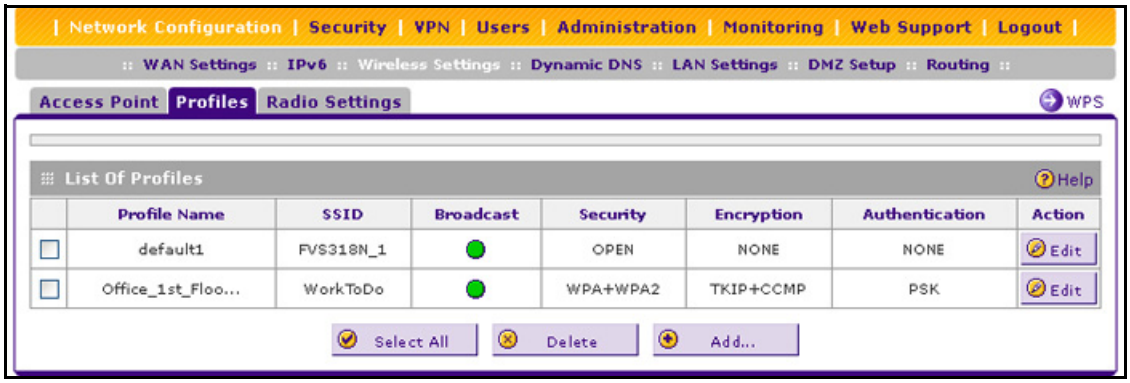


Figure 46.

The following table explains the fields of the Profile screen:

Table 21. Profiles screen settings

Field	Description
Profile Name	The unique name of the security profile that makes it easy to recognize the profile.
SSID	The wireless network name (SSID) for the security profile.
Broadcast	Indicates whether or not the SSID is broadcast. A green circle indicates that the SSID is broadcast; a gray circle indicates that it is not.
Security	The configured security method for the security profile.
Encryption	The configured encryption method for the security profile.
Authentication	The configured authentication method for the security profile.

2. Under the List of Profiles table, click the **Add** table button. The Add Profiles screen displays:

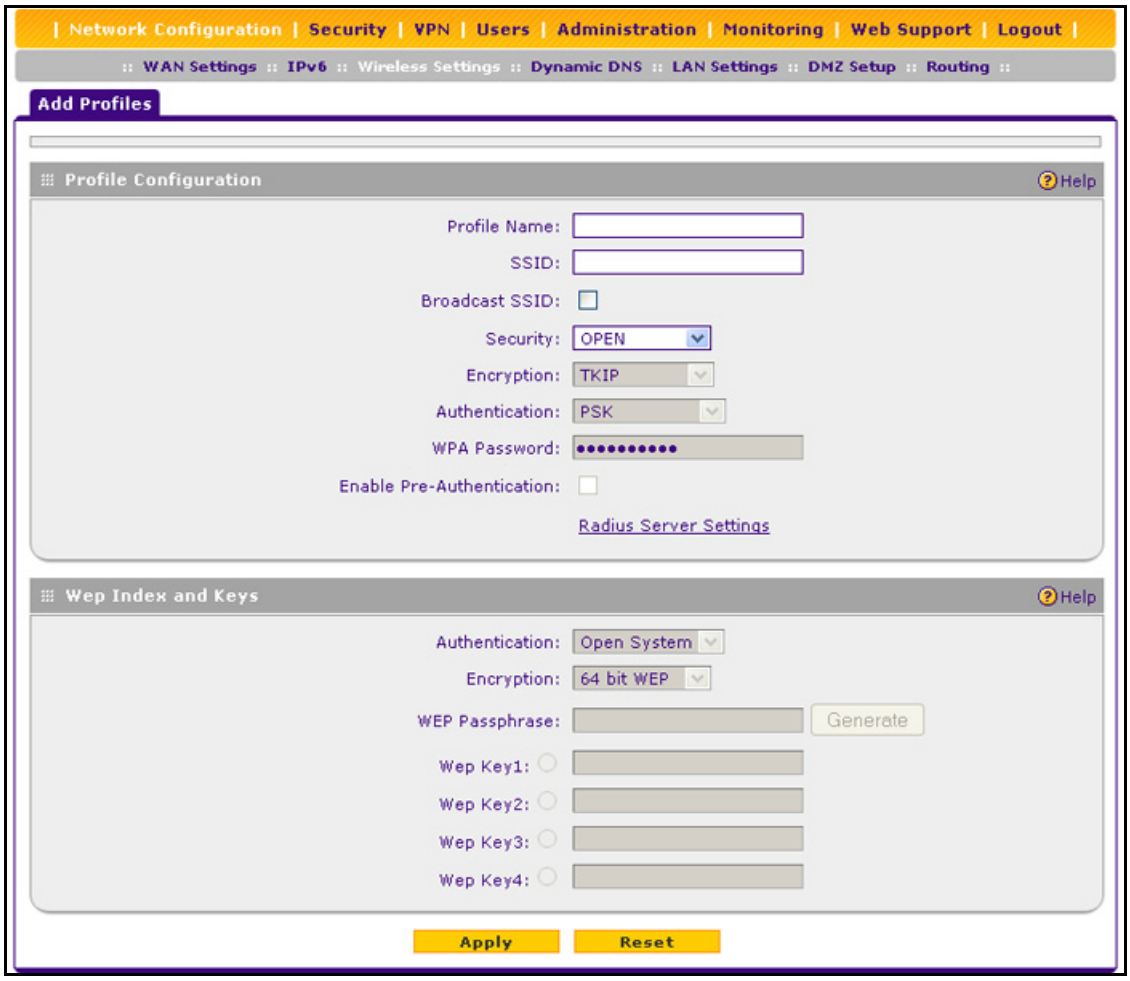


Figure 47.

3. Specify the settings as explained in the following table:

Table 22. Add Profile screen settings

Field	Description
Profile Configuration	
Profile Name	The name for the default wireless security profile is default1. You cannot change this name. For additional profiles, enter a unique name to make it easy to recognize the profile. You can enter a name of up to 32 alphanumeric characters.
SSID	The wireless network name (SSID) for the wireless security profile. The default SSID name is FVS318N_1. You can change this name by entering up to 32 alphanumeric characters. Make sure that additional SSIDs have unique names.

Table 22. Add Profile screen settings (continued)

Field	Description
Broadcast SSID	Select the check box to enable the wireless VPN firewall to broadcast its SSID, allowing wireless stations that have a null (blank) SSID to adopt the wireless VPN firewall's SSID. To prevent the SSID from being broadcast, clear the check box.
Security	**Note:** Before you configure security, you might want to read *Wireless Data Security Options* on page 89. Specify the wireless security by making a selection from the drop-down list: • **OPEN**. This is the default setting. An open system has no authentication and no encryption, and therefore no security configuration. However, you *can* use an open system with encryption. To do so, select **WEP** from the Security drop-down list. In the WEP Index and Keys section of the screen, take the following steps: - Select **Open System** authentication. - Select the encryption. - Enter a passphrase and generate a key, or enter a key manually. • **WEP**. To configure WEP, take the following steps in the WEP Index and Keys section of the screen: - Select **Shared Key** authentication. - Select the encryption. - Enter a passphrase and generate a key, or enter a key manually. • **WPA**. To configure WPA, select the encryption and authentication. The remaining configuration depends on the selected authentication: - For WPA-PSK, select a password. - For WPA with RADIUS, configure the RADIUS server settings. - For WPA with PSK+RADIUS, select a password and configure the RADIUS server settings. • **WPA2**. To configure WPA2, select the encryption and authentication. The remaining configuration depends on the selected authentication: - For WPA2-PSK, select a password. - For WPA2 with RADIUS, configure the RADIUS server settings. As an option, you can enable RADIUS preauthentication. - For WPA2 with PSK+RADIUS, select a password and configure the RADIUS server settings. As an option, you can enable RADIUS preauthentication. • **WPA+WPA2**. To configure WPA, select the encryption and authentication. The remaining configuration depends on the selected authentication: - For WPA+WPA2 with PSK, select a password. - For WPA+WPA2 with RADIUS, configure the RADIUS server settings. - For WPA+WPA2 with PSK+RADIUS, select a password and configure the RADIUS server settings.

Table 22. Add Profile screen settings (continued)

Field	Description
Encryption **Note:** WPA, WPA2, and WPA+WPA2 only.	The encryption that you can select depends on the type of WPA security that you have selected: • **WPA**. You can select the following encryption from the drop-down list: **- TKIP** **- TKIP+CCMP** • **WPA2**. You can select the following encryption from the drop-down list: **- CCMP** **- TKIP+CCMP** • **WPA+WPA2**. The encryption is TKIP+CCMP.
Authentication **Note:** WPA, WPA2, and WPA+WPA2 only.	For WPA, WPA2, and WPA+WPA2 only, specify the authentication by making a selection from the drop-down list: • **PSK** • **RADIUS** • **PSK+RADIUS**
WPA Password **Note:** WPA, WPA2, and WPA+WPA2 only.	For WPA, WPA2, and WPA+WPA2 only, if you have selected PSK or PSK+RADIUS authentication, enter a pre-shared key or password.
Enable Pre-Authentication **Note:** WPA2 only.	For WPA2 only, if you have selected RADIUS authentication, configure preauthentication by selecting the check box. Preauthentication allows a client to roam from one access point to another access point without having to be reauthenticated.
Radius Server Settings **Note:** WPA, WPA2, and WPA+WPA2 only.	For WPA, WPA2, and WPA+WPA2 only, if you have selected RADIUS or PSK+RADIUS authentication, click the **Radius Server Settings** link to configure the RADIUS settings (see *RADIUS Client Configuration* on page 196).
WEP Index and Keys	
Authentication	Specify the authentication by making a selection from the drop-down list: • **Open System**. Select this option to use WEP encryption without authentication. • **Shared Key**. Select this option to use WEP authentication and encryption with a shared key (passphrase).
Encryption	Select the encryption key size by making a selection from the drop-down list: • **64-bit WEP**. Standard WEP encryption, using 40/64-bit encryption. • **128-bit WEP**. Standard WEP encryption, using 104/128-bit encryption.
Passphrase	Enter a passphrase. The passphrase length needs to be between 8 and 63 characters (inclusive). The secret passphrase allows you to automatically generate the keys by clicking **Generate**.

Table 22. Add Profile screen settings (continued)

Field	Description
Encryption Key (Key1–Key4)	Specify the active key by selecting one of the four radio buttons. Only one key can be the active key. Either enter a key manually or generate the key automatically by clicking **Generate**. The length of the key depends on the selected encryption: • **64-bit WEP**. A key length of 5 ASCII or 10 hexadecimal characters. • **128-bit WEP**. A key length of 13 ASCII or 26 hexadecimal characters. **Note:** Wireless stations need to use the key to access the wireless VPN firewall.

4. Click **Apply** to save your settings. The new profile is added to the List of Profiles table.

WARNING!

If you use a wireless computer to configure wireless security settings, you will be disconnected when you click Apply. Reconfigure your wireless computer to match the new settings, or access the wireless VPN firewall from a wired computer to make further changes.

Note: For information about how to configure WPS, see *Configure Wi-Fi Protected Setup* on page 102.

➢ **To edit a security profile:**

1. On the Profiles screen (see *Figure 46* on page 93), click the **Edit** button in the Action column for the security profile that you want to modify. The Edit Profiles screen displays. This screen is identical to the Add Profiles screen.
2. Modify the settings as explained in the previous table.
3. Click **Apply** to save your settings.

Note: If WPS is enabled for the security profile, first disable WPS before you edit the security profile.

➢ **To delete one or more security profiles:**

1. On the Profiles screen (see *Figure 46* on page 93), select the check box to the left of each security profile that you want to delete, or click the **Select All** table button to select all security profiles. (You cannot select the default security profile.)
2. Click the **Delete** table button.

Note: If WPS is enabled for the security profile, first disable WPS before you delete the security profile.

Configure Virtual Access Points

You can configure up to four virtual access points (VAPs) on the wireless VPN firewall. All VAPs can be active simultaneously to accommodate different types of clients. You can assign only a single security profile to each VAP, and the same security profile cannot be assigned to more than one VAP.

Each VAP provides the following features:

- Capability to turn off the VAP during scheduled vacations and office shutdowns, on evenings, or on weekends. This a green feature that allows you to save energy.
- WLAN partitioning to prevent associated wireless clients (using the same VAP) from communicating with each other. This feature is useful for hotspots and other public access situations.
- MAC address access control list that lets you add another level of security.
- Capability to monitor the VAP and its connected clients.

➢ **To add a VAP:**

1. Select **Network Configuration > Wireless Settings > Access Point**. The Access Point screen displays. (The following figure shows some examples.)

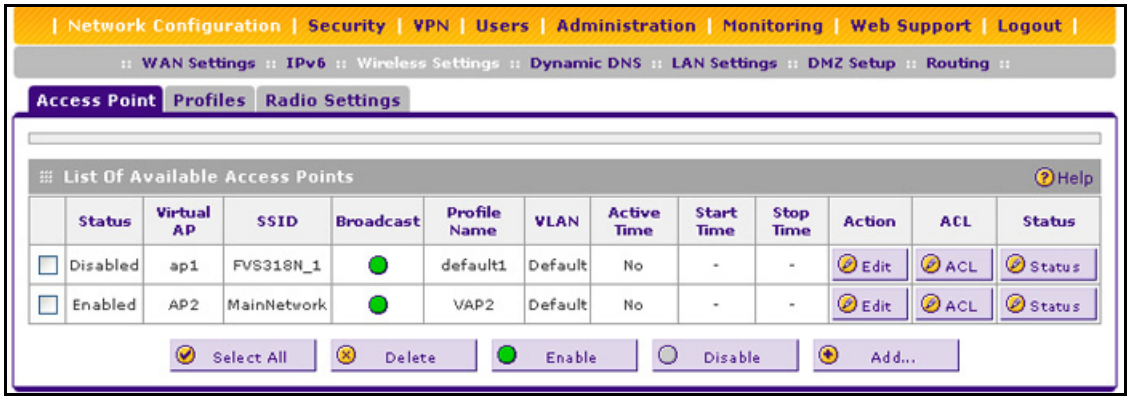


Figure 48.

The following table explains the fields of the Access Point screen:

Table 23. Access Point screen settings

Item	Description
Status	The status of the VAP (Enabled or Disabled).
Virtual AP	The name of the VAP.
SSID	The wireless network name (SSID) for the security profile that is allocated to the VAP.
Broadcast	Indicates whether or not the SSID is broadcast. A green circle indicates that the SSID is broadcast; a gray circle indicates that it is not.
Profile Name	The security profile that is allocated to the VAP.
VLAN	The VLAN to which the VAP is allocated.
Active Time	Indicates whether or not the timer for the VAP is activated (No or Yes).
Start Time	The start time for the timer.
Stop Time	The stop time for the timer.

2. Under the List Of Available Access Points table, click the **Add** table button. The Add Access Point screen displays:

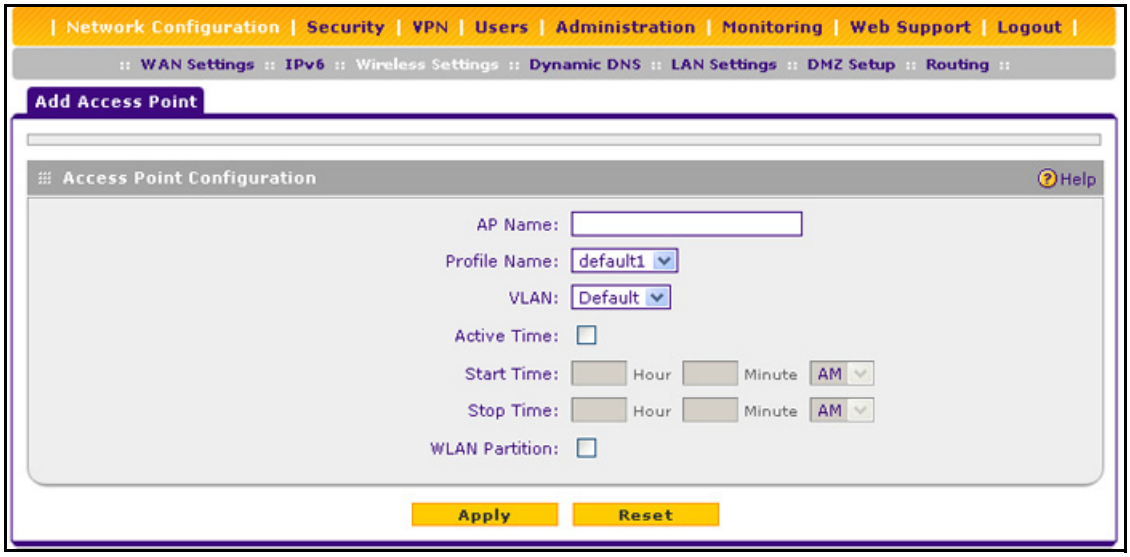


Figure 49.

3. Specify the settings as explained in the following table:

Table 24. Add Access Point screen settings

Settings	Description
AP Name	The name for the default VAP is ap1. You cannot change this name. For additional VAPs, enter a unique name to make it easy to recognize the profile. You can enter a value of up to 32 alphanumeric characters.
Profile Name	From the drop-down list, select the profile that should be allocated to the VAP.
VLAN	From the drop-down list, select the VLAN to which the VAP should be allocated.
Active Time	To enable the timer, select the **Active Time** check box. When the timer is enabled, the VAP is turned off from the start time until the stop time. To disable the timer, clear the check box.
Start Time	Specify the start hour in the Hours field and the start minute in the Minutes field, and then select **AM** or **PM** from the drop-down list.
Stop Time	Specify the stop hour in the Hours field and the stop minute in the Minutes field, and then select **AM** or **PM** from the drop-down list.
WLAN Partition	To enable wireless client separation and prevent wireless clients that are connected to this VAP from communicating with each other, select the **WLAN Partition** check box. The disable wireless client separation, clear the check box. By default, WLAN partition is disabled.

4. Click **Apply** to save your settings. The new VAP is added to the List Of Available Access Points table.

➢ **To enable or disable one or more VAPs:**

1. On the Access Point screen (see *Figure 48* on page 98), select the check box to the left of each VAP that you want to enable or disable, or click the **Select All** table button to select all VAPs.
2. Click one of the following table buttons:
   - **Enable**. Enables the VAP or VAPs and allows wireless clients to make a connection.
   - **Disable**. Disables the VAP or VAPs and prevents wireless clients from making a connection.

➢ **To edit a VAP:**

1. On the Access Point screen (see *Figure 48* on page 98), click the **Edit** button in the Action column for the VAP that you want to modify. The Edit Access Point screen displays. This screen is identical to the Add Access Point screen.
2. Modify the settings as explained in the previous table.
3. Click **Apply** to save your settings.

➢ **To delete one or more VAPs:**

1. On the Access Point screen (see *Figure 48* on page 98), select the check box to the left of each VAP that you want to delete, or click the **Select All** table button to select all VAPs. (You cannot select the default VAP.)
2. Click the **Delete** table button.

Restrict Wireless Access by MAC Address

For increased security, you can restrict access to an SSID by allowing access to only specific computers or wireless stations based on their MAC addresses. You can restrict access to only trusted computers so that unknown computers cannot wirelessly connect to the wireless VPN firewall. MAC address filtering adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed.

Note: For wireless adapters, you can usually find the MAC address printed on the wireless adapter.

➢ **To allow or restrict access based on MAC addresses:**

1. On the Access Point screen (see *Figure 48* on page 98), click the **ACL** button in the Action column for the VAP for which you want to set up access control. The MAC Address Filtering screen displays. (The following figure shows some examples.)

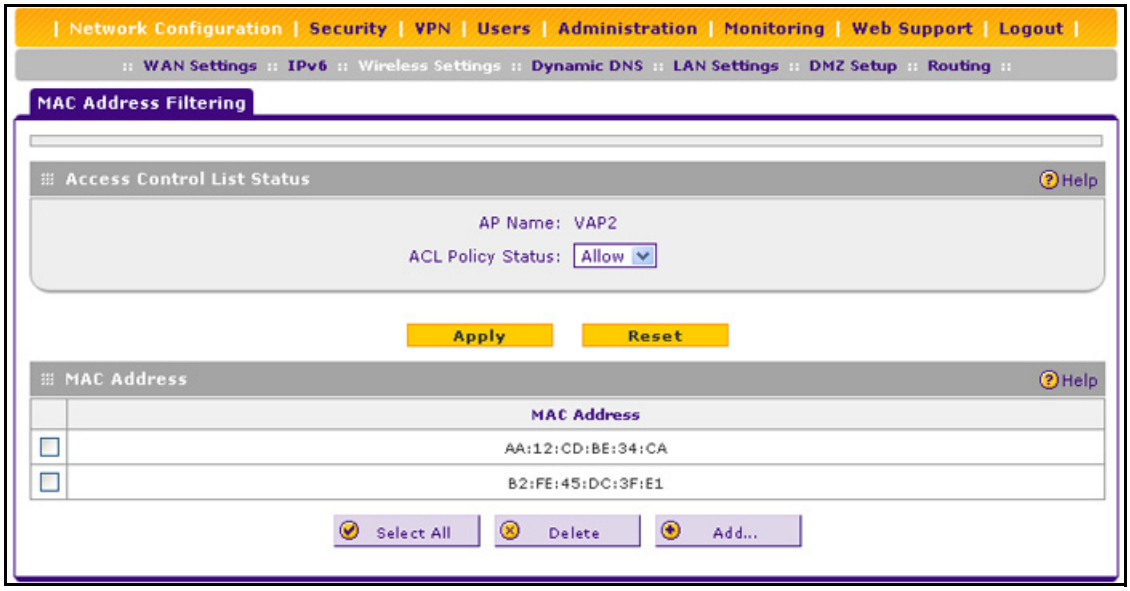


Figure 50.

2. Click **Add** to open the MAC Address screen (not shown in this manual).
3. Enter a MAC address in the MAC Address field.
4. Click **Apply** to add the MAC address to the MAC Address table on the MAC Address Filtering screen.

5. Repeat *step 2* through *step 4* for any other MAC address that you want to add to the MAC Address table.
6. From the ACL Policy Status drop-down list, select if access control is enabled, and if so, how the MAC addresses in the MAC Address table are treated:
   - **Open**. Access control is disabled. All MAC addresses, including the ones in the MAC Address table, are allowed access.
   - **Allow**. Only the MAC addresses in the MAC Address table are allowed access. All other MAC addresses are denied access.
   - **Deny**. The MAC addresses in the MAC Address table are denied access. All other MAC addresses are allowed access.
7. Click **Apply** to save your settings.

WARNING!

When configuring the wireless VPN firewall from a wireless computer whose MAC address is not in the access control list and when the ACL policy status is set to deny access, you will lose your wireless connection when you click Apply. You then need to access the wireless VPN firewall from a wired computer or from a wireless computer that is on the access control list to make any further changes.

➢ **To remove one or more MAC addresses from the table:**

1. In the MAC Address table, select the check box to the left of each MAC address that you want to delete, or click the **Select All** table button to select all MAC addresses.
2. Click the **Delete** table button.

Configure Wi-Fi Protected Setup

Push 'N' Connect using Wi-Fi Protected Setup™ (WPS) allows you to connect computers to a secure wireless network with WPA or WPA2 wireless security. The wireless VPN firewall automatically sets security for each computer or device that uses WPS to join the wireless network. To use WPS, make sure that your wireless devices are Wi-Fi certified and support WPS. NETGEAR products that use WPS call it Push 'N' Connect.

You can use a WPS button or the wireless router interface method to add wireless computers and devices to your wireless network.

Note: For a list of other Wi-Fi-certified products available from NETGEAR, go to *http://www.wi-fi.org*.

➢ **To enable WPS and initiate the WPS process on the wireless VPN firewall:**

1. Select **Network Configuration > Wireless Settings > Profiles**. The Profiles screen displays (see *Figure 46* on page 93).
2. Click the **WPS** option arrow in the upper right of the Radio Settings screen. The WPS screen displays.

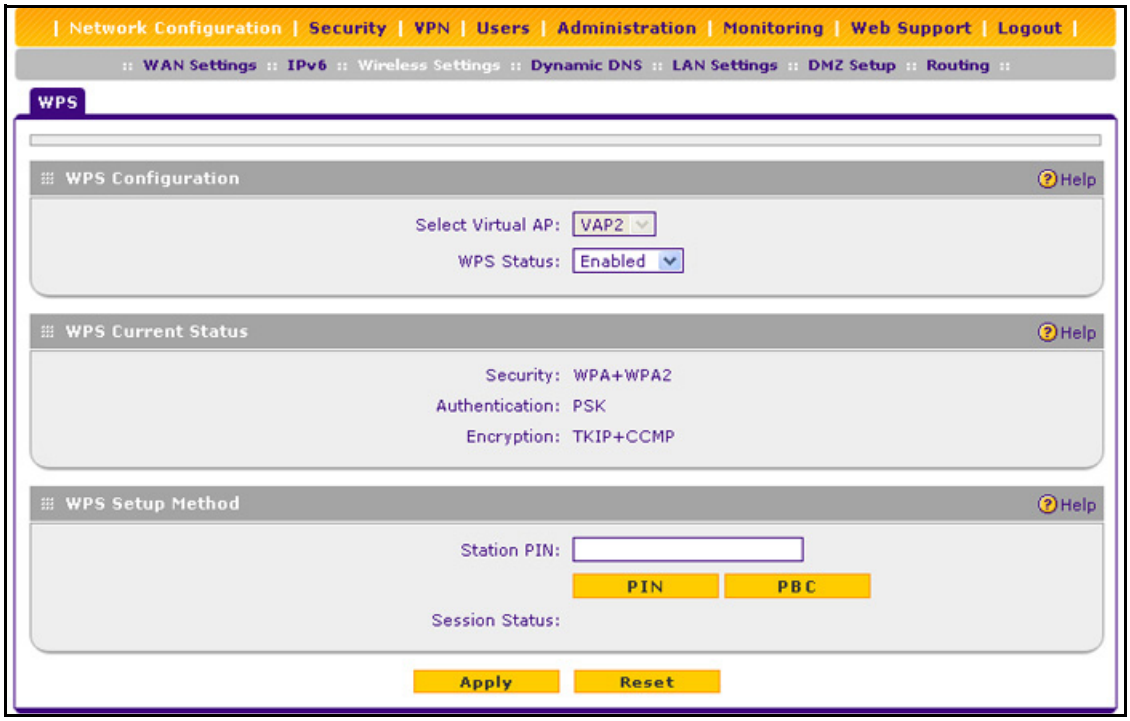


Figure 51.

3. From the WPS Status drop-down list, select **Enabled** to enable the WPS feature.
4. Click **Apply** to save your changes.

Note: *The Select Virtual AP, Security, Authentication, and Encryption fields are nonconfigurable fields that are for information only.*

5. In the WPS Setup Method section of the screen, use one of the following methods to initiate the WPS process for a wireless device:
   - PIN method:
     a. Collect the pin of the wireless device.
     b. In the Station PIN field, enter the pin.
     c. Click the **PIN** button.
   - Push button configuration (PBC) method:
     a. Click the **PBC** button.
     b. Within 2 minutes, press the **WPS** button on your wireless device to enable the device to connect the access point of the wireless VPN firewall, or follow the WPS instructions that came with the device.

With either method, the wireless VPN firewall tries to communicate with the wireless device, set the wireless security for the wireless device, and allow it to join the wireless network.

Note: There is no physical WPS push button on the wireless VPN firewall.

Configure Advanced Radio Settings

➢ **To configure advanced radio settings:**

1. Select **Network Configuration > Wireless Settings > Radio Settings**. The Radio Settings screen displays (see *Figure 44* on page 86).
2. Click the **Advanced** option arrow in the upper right of the Radio Settings screen. The Advanced Wireless screen displays:

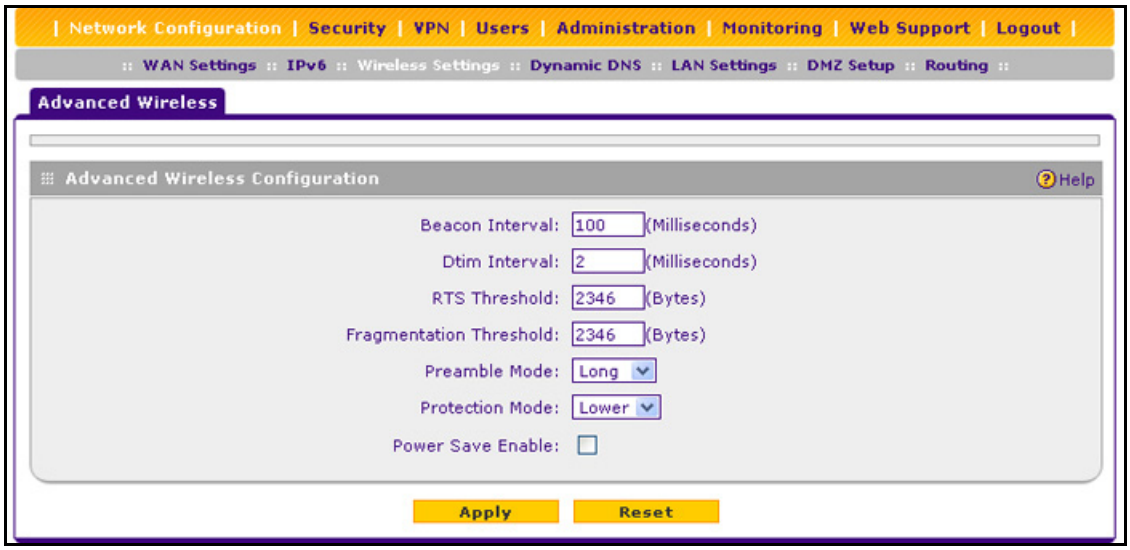

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
WAN Settings :: IPv6 :: Wireless Settings :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing
Advanced Wireless
Advanced Wireless Configuration
Help
Beacon Interval: 100 (Milliseconds)
Dtim Interval: 2 (Milliseconds)
RTS Threshold: 2346 (Bytes)
Fragmentation Threshold: 2346 (Bytes)
Preamble Mode: Long
Protection Mode: Lower
Power Save Enable:
Apply
Reset

Figure 52.

3. Specify the settings as explained in the following table:

Table 25. Advanced Wireless screen settings

Setting	Description
Beacon Interval	Enter an interval between 40 ms and 3500 ms for each beacon transmission, which allows the wireless VPN firewall to synchronize the wireless network. The default setting is 100.
DTIM Interval	Enter the Delivery Traffic Indication Message (DTIM) interval, also referred to as the data beacon rate, which indicates the period for the beacon DTIM in multiples of beacon intervals. This value needs to be between 1 and 255. The default setting is 2.

Table 25. Advanced Wireless screen settings (continued)

Setting	Description
RTS Threshold	Enter the Request to Send (RTS) threshold. The default setting is 2346 bytes. If the packet size is equal to or less than the RTS threshold, the wireless VPN firewall uses the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) mechanism, and the data frame is transmitted immediately after the silence period. If the packet size is larger than the RTS threshold, the wireless VPN firewall uses the CSMA with Collision Avoidance (CSMA/CA) mechanism. In this situation, the transmitting station sends an RTS packet to the receiving station and waits for the receiving station to return a Clear to Send (CTS) packet before sending the actual packet data. This method improves the performance but reduces the throughput.
Fragmentation Threshold	Enter the maximum packet size that is used for the fragmentation of data packets. Packets that are larger than the specified fragmentation length are broken up into smaller packets before being transmitted. The fragmentation threshold needs to be an even number. The default setting is 2346 bytes.
Preamble Mode	Specify the preamble mode by making a selection from the drop-down list: • **Long**. A long transmit preamble might provide a more reliable connection or a slightly longer range. This is the default mode. • **Short**. A short transmit preamble gives better performance.
Protection Mode	Specify the Clear to Send (CTS)-to-self protection mode by making a selection from the drop-down list: • **Lower**. CTS-to-self protection mode is disabled. This is the default mode. • **Upper**. CTS-to-self protection mode is enabled. This mode increases the performance but reduces the throughput slightly.
Power Save Enable	To enable the Wi-Fi Multimedia (WMM) Powersave feature, select the **Power Save Enable** check box. This feature saves power for battery-powered equipment by increasing the efficiency and flexibility of data transmission. Clear the check box to disable the feature, which is the default setting.

4. Click **Apply** to save your settings.

Test Basic Wireless Connectivity

After you have configured the wireless VPN firewall as explained in the previous sections, test your wireless clients for wireless connectivity before you place the wireless VPN firewall at its permanent position.

➢ **To test for wireless connectivity:**

1. Configure the 802.11b/g/n wireless clients so that they all have the same SSID that you have configured on the wireless VPN firewall. Make sure that the wireless mode on the wireless VPN firewall supports the wireless capacity of the wireless clients. (For example, 802.11b-compliant devices cannot connect to the wireless VPN firewall if the wireless mode is set to ng.)

2. Verify that your wireless clients have a link to the wireless VPN firewall. If you have enabled the DHCP server on the wireless VPN firewall (see *Configure a VLAN Profile* on page 51 (for IPv4) and *Configure IPv6 LAN Settings* on page 64), verify that your wireless clients are able to obtain an IP address through DHCP from the wireless VPN firewall.
3. Verify network connectivity by using a browser such as Internet Explorer 6.0 or later or Mozilla Firefox 1.5 or later to browse the Internet, or check for file and printer access on your network.

If you have trouble connecting to the wireless VPN firewall, try to connect without security by selecting **OPEN** from the Security drop-down list on the Edit Profiles screen for the profile that is allocated to the access point. If that does not help you to solve the connection problem, see *Chapter 11, Troubleshooting*.

IPv4 Firewall Protection

5

This chapter describes how to use the IPv4 firewall features of the wireless VPN firewall to protect your network. This chapter contains the following sections:

- *About IPv4 Firewall Protection*
- *Rules to Block or Allow Specific Kinds of Traffic*
- *Configure Other Firewall Features*
- *Services, Bandwidth Profiles, and QoS Profiles*
- *Configure Content Filtering*
- *Set a Schedule to Block or Allow Specific Traffic*
- *Enable Source MAC Filtering*
- *Set Up IP/MAC Bindings*
- *Configure Port Triggering*
- *Configure Universal Plug and Play*

About IPv4 Firewall Protection

A firewall protects one network (the trusted network, such as your LAN) from another (the untrusted network, such as the Internet), while allowing communication between the two. You can further segment keyword blocking to certain known groups. For information about how to set up LAN groups, see *Manage IPv4 Groups and Hosts (IPv4 LAN Groups)* on page 59.

Note: In this release, the wireless VPN firewall supports firewall security for IPv4 traffic only; IPv6 addresses are ignored by the firewall. By themselves IPv6 addresses provide a much higher level of security than IPv4 addresses, and future releases will support IPv6 firewall features.

A firewall incorporates the functions of a Network Address Translation (NAT) router, protects the trusted network from hacker intrusions or attacks, and controls the types of traffic that

can flow between the two networks. Unlike simple NAT routers, a firewall uses a process called Stateful Packet Inspection to protect your network from attacks and intrusions. NAT performs a very limited stateful inspection in that it considers whether the incoming packet is in response to an outgoing request, but true Stateful Packet Inspection goes far beyond NAT.

Administrator Tips

Consider the following operational items:

1. As an option, you can enable remote management if you have to manage distant sites from a central location (see *Configure Authentication Domains, Groups, and Users* on page 247 and *Configure Remote Management Access* on page 278).
2. Although rules are the basic way of managing the traffic through your system (see *Rules to Block or Allow Specific Kinds of Traffic* on page 108), you can further refine your control using the following features and capabilities of the wireless VPN firewall:
   - Groups and hosts (see *Manage IPv4 Groups and Hosts (IPv4 LAN Groups)* on page 59)
   - Services (see *Service-Based Rules* on page 109)
   - Schedules (see *Set a Schedule to Block or Allow Specific Traffic* on page 146)
   - Allowing or blocking sites (see *Configure Content Filtering* on page 142)
   - Source MAC filtering (see *Enable Source MAC Filtering* on page 147)
   - Port triggering (see *Configure Port Triggering* on page 151)
3. Some firewall settings might affect the performance of the wireless VPN firewall. For more information, see *Performance Management* on page 270.
4. The firewall logs can be configured to log and then email denial of access, general attack, and other information to a specified email address. For information about how to configure logging and notifications, see *Configure Logging, Alerts, and Event Notifications* on page 293.

Rules to Block or Allow Specific Kinds of Traffic

Firewall rules are used to block or allow specific traffic passing through from one side to the other. You can configure up to 300 inbound rules *plus* up to 300 outbound rules on the wireless VPN firewall (see the following table). Inbound rules (WAN to LAN) restrict access by outsiders to private resources, selectively allowing only specific outside users to access specific resources. Outbound rules (LAN to WAN) determine what outside resources local users can have access to.

A firewall has two default rules, one for inbound traffic and one for outbound. The default rules of the wireless VPN firewall are:

- **Inbound**. Block all access from outside except responses to requests from the LAN side.
- **Outbound**. Allow all access from the LAN side to the outside.

The firewall rules for blocking and allowing traffic on the wireless VPN firewall can be applied to LAN WAN traffic, DMZ WAN traffic, and LAN DMZ traffic.

Table 26. Number of supported firewall rule configurations

Traffic rule	Maximum number of outbound rules	Maximum number of inbound rules	Maximum number of supported rules
LAN WAN	200	200	400
DMZ WAN	50	50	100
LAN DMZ	50	50	100
Total Rules	300	300	600

Service-Based Rules

The rules to block traffic are based on the traffic's category of service:

- **Outbound rules (service blocking)**. Outbound traffic is usually allowed unless the firewall is configured to disallow it.
- **Inbound rules (port forwarding)**. Inbound traffic is usually blocked by the firewall unless the traffic is in response to a request from the LAN side. The firewall can be configured to allow this otherwise blocked traffic.
- **Customized services**. Additional services can be added to the list of services in the factory defaults list. These added services can then have rules defined for them to either allow or block that traffic (see *Add Customized Services* on page 136).
- **Quality of Service (QoS) priorities**. Each service has its own native priority that impacts its quality of performance and tolerance for jitter or delays. You can change the QoS priority, which changes the traffic mix through the system (see *Preconfigured Quality of Service Profiles* on page 141).

Outbound Rules (Service Blocking)

The wireless VPN firewall allows you to block the use of certain Internet services by PCs on your network. This is called service blocking or port filtering.

Note: See *Enable Source MAC Filtering* on page 147 for yet another way to block outbound traffic from selected PCs that would otherwise be allowed by the firewall.

WARNING!

Allowing inbound services opens security holes in your wireless VPN firewall. Enable only those ports that are necessary for your network.

The following table describes the fields that define the rules for outbound traffic and that are common to most Outbound Service screens (see *Figure 55* on page 118, *Figure 58* on page 121, and *Figure 61* on page 124).

The steps to configure outbound rules are described in the following sections:

- *Set LAN WAN Rules*
- *Create DMZ WAN Rules*
- *Create LAN DMZ Rules*

Table 27. Outbound rules overview

Setting	Description
Service	The service or application to be covered by this rule. If the service or application does not display in the list, you need to define it using the Services screen (see *Add Customized Services* on page 136).
Action	The action for outgoing connections covered by this rule: • **BLOCK always** • **BLOCK by schedule, otherwise allow** • **ALLOW always** • **ALLOW by schedule, otherwise block** **Note:** Any outbound traffic that is not blocked by rules you create is allowed by the default rule. **Note:** ALLOW rules are useful only if the traffic is already covered by a BLOCK rule. That is, you wish to allow a subset of traffic that is currently blocked by another rule.
Select Schedule	The time schedule (that is, Schedule1, Schedule2, or Schedule3) that is used by this rule. • This drop-down list is activated only when BLOCK by schedule, otherwise allow or ALLOW by schedule, otherwise block is selected as the action. • Use the Schedule screen to configure the time schedules (see *Set a Schedule to Block or Allow Specific Traffic* on page 146).
LAN Users	The settings that determine which computers on your network are affected by this rule. The options are: • **Any**. All PCs and devices on your LAN. • **Single address**. Enter the required address in the Start field to apply the rule to a single device on your LAN. • **Address range**. Enter the required addresses in the Start and Finish fields to apply the rule to a range of devices. • **Group**. Select the LAN group to which the rule applies. Use the LAN Groups screen to assign PCs to groups (see *Manage the Network Database* on page 60).
WAN Users	The settings that determine which Internet locations are covered by the rule, based on their IP address. The options are: • **Any**. All Internet IP address are covered by this rule. • **Single address**. Enter the required address in the Start field. • **Address range**. Enter the required addresses the Start and Finish fields.

Table 27. Outbound rules overview (continued)

Setting	Description
DMZ Users	The settings that determine which DMZ computers on the DMZ network are affected by this rule. The options are: • **Any**. All PCs and devices on your DMZ network. • **Single address**. Enter the required address in the Start field to apply the rule to a single PC on the DMZ network. • **Address range**. Enter the required addresses in the Start and Finish fields to apply the rule to a range of DMZ computers.
QoS Priority	The priority assigned to IP packets of this service. The priorities are defined by Type of Service (ToS) in the Internet Protocol Suite standards, RFC 1349. The QoS profile determines the priority of a service, which, in turn, determines the quality of that service for the traffic passing through the firewall. The wireless VPN firewall marks the Type of Service (ToS) field as defined in the QoS profiles that you create. For more information, see *Preconfigured Quality of Service Profiles* on page 141. **Note:** The wireless VPN firewall has preconfigured default QoS profiles; you cannot configure the QoS profiles. A QoS profile can become active only when you apply it to a nonblocking inbound or outbound firewall rule.
Bandwidth Profile	Bandwidth limiting determines the way in which the data is sent to and from your host. The purpose of bandwidth limiting is to provide a solution for limiting the outgoing and incoming traffic, thus preventing the LAN users from consuming all the bandwidth of the Internet link. For more information, see *Create Bandwidth Profiles* on page 139. For outbound traffic, you can configure bandwidth limiting only on the WAN interface for a LAN WAN rule. **Note:** Bandwidth limiting does not apply to the DMZ interface.
Log	The setting that determines whether packets covered by this rule are logged. The options are: • **Always**. Always log traffic considered by this rule, whether it matches or not. This is useful when you are debugging your rules. • **Never**. Never log traffic considered by this rule, whether it matches or not.
NAT IP	The setting that specifies whether the source address of the outgoing packets on the WAN should be assigned the address of the WAN interface or the address of a different interface. You can specify these settings only for outbound traffic of the WAN interface. The options are: • **WAN Interface Address**. All the outgoing packets on the WAN are assigned to the address of the specified WAN interface. • **Single Address**. All the outgoing packets on the WAN are assigned to the specified IP address, for example, a secondary WAN address that you have configured. **Note:** The NAT IP option is available only when the WAN mode is NAT. The IP address specified should fall under the WAN subnet.

Inbound Rules (Port Forwarding)

If you have enabled Network Address Translation (NAT), your network presents only *one* IP address to the Internet, and outside users cannot directly access any of your local computers (LAN users). (For information about configuring NAT, see *Network Address Translation* on page 31.) However, by defining an inbound rule you can make a local server (for example, a web server or game server) visible and available to the Internet. The rule informs the firewall to direct inbound traffic for a particular service to one local server based on the destination port number. This process is also known as port forwarding.

Whether or not DHCP is enabled, how the PC accesses the server's LAN address impacts the inbound rules. For example:

- If your external IP address is assigned dynamically by your ISP (DHCP enabled), the IP address might change periodically as the DHCP lease expires. Consider using Dyamic DNS so that external users can always find your network (see *Configure Dynamic DNS* on page 40).
- If the IP address of the local server PC is assigned by DHCP, it might change when the PC is rebooted. To avoid this, use the Reserved (DHCP Client) feature in the LAN Groups screen to keep the PC's IP address constant (see *Set Up Address Reservation* on page 64).
- Local PCs need to access the local server using the PCs' local LAN address. Attempts by local PCs to access the server using the external WAN IP address will fail.

Note: See *Configure Port Triggering* on page 151 for yet another way to allow certain types of inbound traffic that would otherwise be blocked by the firewall.

Note: The wireless VPN firewall always blocks denial of service (DoS) attacks. A DoS attack does not attempt to steal data or damage your PCs, but overloads your Internet connection so you cannot use it (that is, the service becomes unavailable).

Note: When the Block TCP Flood and Block UDP Flood check boxes are selected on the Attack Checks screen (see *Attack Checks* on page 132), multiple concurrent connections of the same application from one host or IP address (such as multiple DNS queries from one PC) trigger the wireless VPN firewall's DoS protection.

The following table describes the fields that define the rules for inbound traffic and that are common to most Inbound Service screens (see *Figure 56* on page 119, *Figure 59* on page 122, and *Figure 62* on page 125).

The steps to configure inbound rules are described in the following sections:

- *Set LAN WAN Rules*
- *Create DMZ WAN Rules*
- *Create LAN DMZ Rules*

Table 28. Inbound rules overview

Setting	Description
Service	The service or application to be covered by this rule. If the service or application does not display in the list, you need to define it using the Services screen (see *Add Customized Services* on page 136).
Action	The action for outgoing connections covered by this rule: • **BLOCK always** • **BLOCK by schedule, otherwise allow** • **ALLOW always** • **ALLOW by schedule, otherwise block** **Note:** Any inbound traffic that is not blocked by rules you create is allowed by the default rule.
Select Schedule	The time schedule (that is, Schedule1, Schedule2, or Schedule3) that is used by this rule. • This drop-down list is activated only when BLOCK by schedule, otherwise allow or ALLOW by schedule, otherwise block is selected as the action. • Use the Schedule screen to configure the time schedules (see *Set a Schedule to Block or Allow Specific Traffic* on page 146).
Send to LAN Server	The LAN server address determines which computer on your network is hosting this service rule. (You can also translate this address to a port number.) The options are: • **Single address**. Enter the required address in the Start field to apply the rule to a single device on your LAN. • **Address range**. Enter the required addresses in the Start and Finish fields to apply the rule to a range of devices.
Send to DMZ Server	The DMZ server address determines which computer on your network is hosting this service rule. (You can also translate this address to a port number.)
Translate to Port Number	If you want to assign the LAN server or DMZ server to a specific port, you can enable this setting and specify a port number.
WAN Destination IP Address	The setting that determines the destination IP address applicable to incoming traffic. This is the public IP address that maps to the internal LAN server. This can be either the address of the WAN interface or another public IP address. You also have the option to enter an address range. Enter the required addresses in the Start and Finish fields to apply the rule to a range of devices.

Table 28. Inbound rules overview (continued)

Setting	Description
LAN Users	These settings apply to a LAN WAN inbound rule when the WAN mode is classical routing, and determine which computers on your network are affected by this rule. The options are: • **Any**. All PCs and devices on your LAN. • **Single address**. Enter the required address in the Start field to apply the rule to a single device on your LAN. • **Address range**. Enter the required addresses in the Start and Finish fields to apply the rule to a range of devices. • **Group**. Select the LAN group to which the rule applies. Use the LAN Groups screen to assign PCs to groups (see *Manage the Network Database* on page 60). • For LAN WAN inbound rules, this field is not applicable when the WAN mode is NAT because your network presents only *one* IP address to the Internet.
WAN Users	The settings that determine which Internet locations are covered by the rule, based on their IP address. The options are: • **Any**. All Internet IP address are covered by this rule. • **Single address**. Enter the required address in the Start field. • **Address range**. Enter the required addresses in the Start and Finish fields.
DMZ Users	The settings that determine which DMZ computers on the DMZ network are affected by this rule. The options are: • **Any**. All PCs and devices on your DMZ network. • **Single address**. Enter the required address in the Start field to apply the rule to a single PC on the DMZ network. • **Address range**. Enter the required addresses in the Start and Finish fields to apply the rule to a range of DMZ computers. **Note:** For DMZ WAN inbound rules, this field is not applicable when the WAN mode is NAT because your network presents only *one* IP address to the Internet.
Log	The setting that determines whether packets covered by this rule are logged. The options are: • **Always**. Always log traffic considered by this rule, whether it matches or not. This is useful when you are debugging your rules. • **Never**. Never log traffic considered by this rule, whether it matches or not.
Bandwidth Profile	Bandwidth limiting determines the way in which the data is sent to and from your host. The purpose of bandwidth limiting is to provide a solution for limiting the outgoing and incoming traffic, thus preventing the LAN users from consuming all the bandwidth of the Internet link. For more information, see *Create Bandwidth Profiles* on page 139. For inbound traffic, you can configure bandwidth limiting only on the LAN interface for a LAN WAN rule. Bandwidth limiting does not apply to the DMZ interface.

Note: Some residential broadband ISP accounts do not allow you to run any server processes (such as a web or FTP server) from your location. Your ISP might periodically check for servers and might suspend your account if it discovers any active servers at your location. If you are unsure, see the acceptable use policy of your ISP.

Order of Precedence for Rules

As you define a new rule, it is added to a table in a Rules screen as the last item in the list, as shown in the LAN WAN Rules screen example in the following figure:

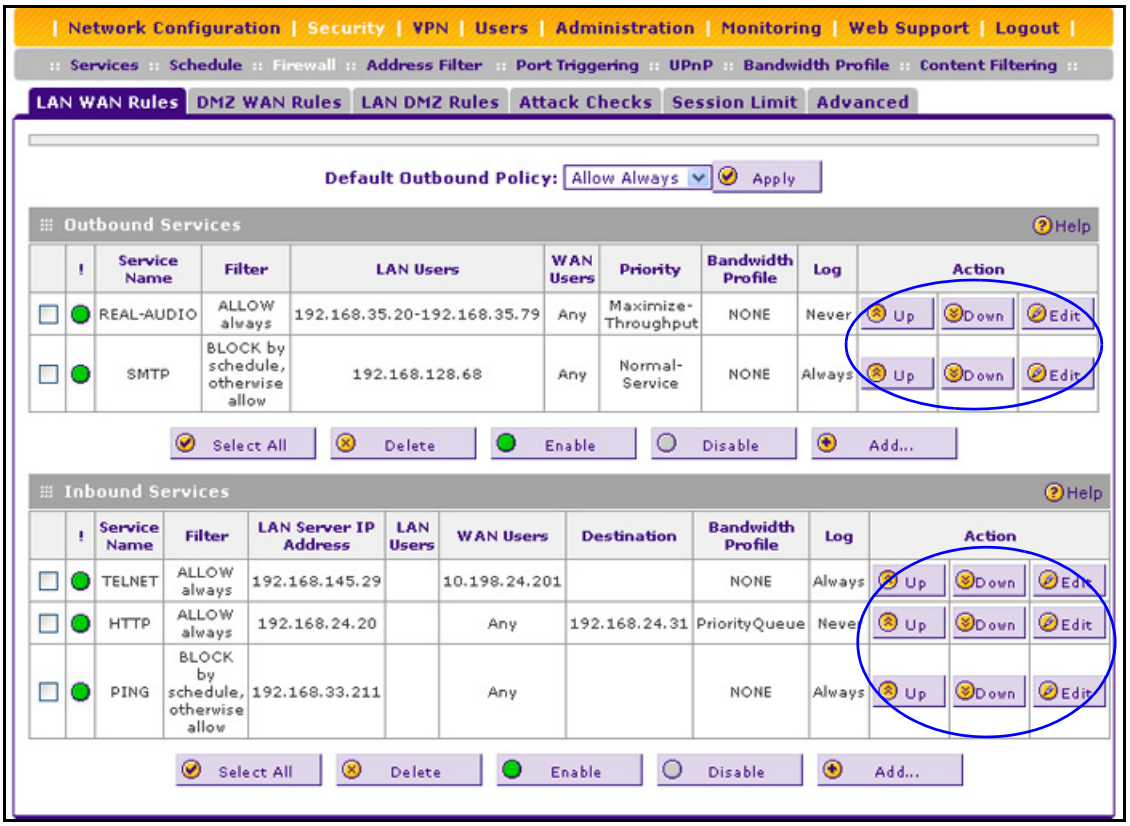


Figure 53.

For any traffic attempting to pass through the firewall, the packet information is subjected to the rules in the order shown in the Rules table, beginning at the top and proceeding to the bottom. In some cases, the order of precedence of two or more rules might be important in determining the disposition of a packet. For example, you should place the most strict rules at the top (those with the most specific services or addresses). The Up and Down table buttons in the Action column allow you to relocate a defined rule to a new position in the table.

Set LAN WAN Rules

The default outbound policy is to allow all traffic to the Internet to pass through. Firewall rules can then be applied to block specific types of traffic from going out from the LAN to the Internet (outbound). This feature is also referred to as service blocking. You can change the default policy of Allow Always to Block Always to block all outbound traffic, which then allows you to enable only specific services to pass through the wireless VPN firewall.

➢ **To change the default outbound policy:**

1. Select **Security > Firewall**. The Firewall submenu tabs display, with the LAN WAN Rules screen in view.
2. Next to Default Outbound Policy, select **Block Always** from the drop-down list.
3. Next to the drop-down list, click the **Apply** table button.

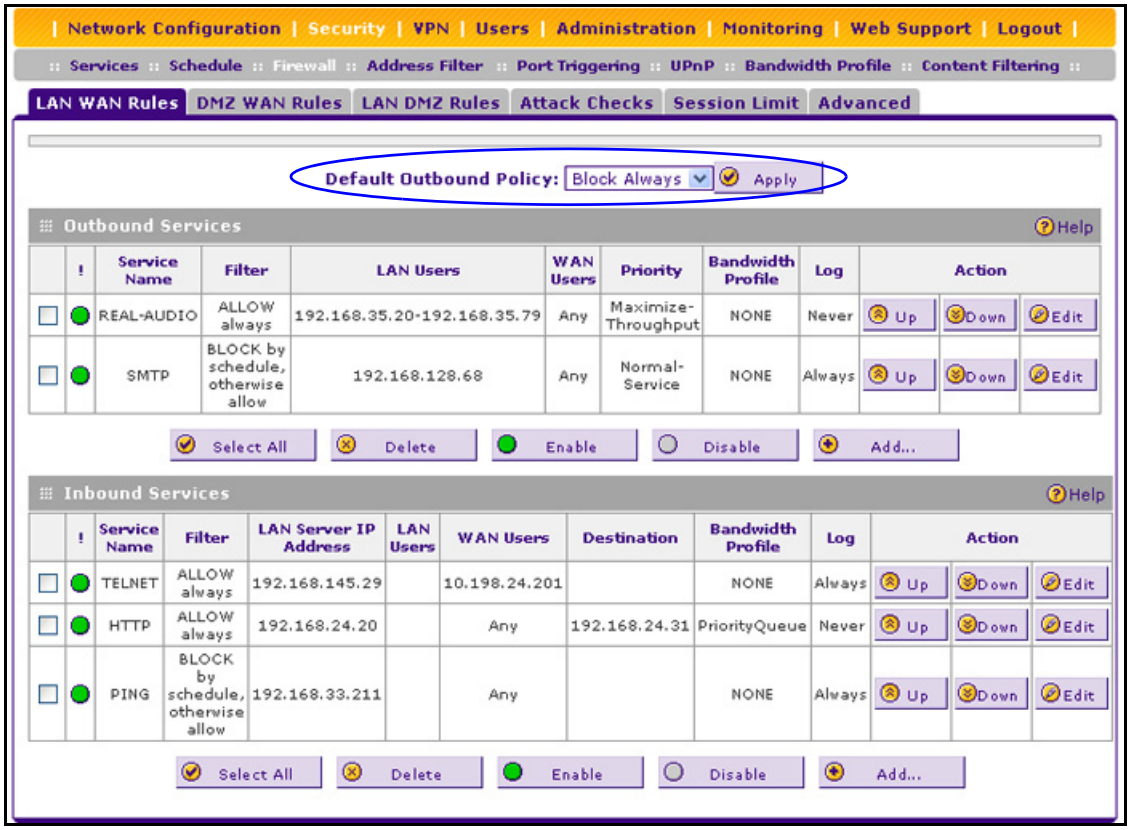

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering
LAN WAN Rules
DMZ WAN Rules
LAN DMZ Rules
Attack Checks
Session Limit
Advanced
Default Outbound Policy: Block Always
Apply
Outbound Services
Help
! Service Name Filter LAN Users WAN Users Priority Bandwidth Profile Log Action
REAL-AUDIO ALLOW always 192.168.35.20-192.168.35.79 Any Maximize-Throughput NONE Never Up Down Edit
SMTP BLOCK by schedule, otherwise allow 192.168.128.68 Any Normal-Service NONE Always Up Down Edit
Select All
Delete
Enable
Disable
Add...
Inbound Services
Help
! Service Name Filter LAN Server IP Address LAN Users WAN Users Destination Bandwidth Profile Log Action
TELNET ALLOW always 192.168.145.29 10.198.24.201 NONE Always Up Down Edit
HTTP ALLOW always 192.168.24.20 Any 192.168.24.31 PriorityQueue Never Up Down Edit
PING BLOCK by schedule, otherwise allow 192.168.33.211 Any NONE Always Up Down Edit
Select All
Delete
Enable
Disable
Add...

Figure 54.

To make changes to an existing outbound or inbound service rule, in the Action column to the right of to the rule, click one of the following table buttons:

- **Up**. Moves the rule up one position in the table rank.
- **Down**. Moves the rule down one position in the table rank.
- **Edit**. Allows you to make any changes to the definition of an existing rule. Depending on your selection, either the Edit LAN WAN Outbound Service screen (identical to *Figure 55*

on page 118) or Edit LAN WAN Inbound Service screen (identical to *Figure 56* on page 119) displays, containing the data for the selected rule.

➢ **To enable, disable, or delete one or more rules:**

1. select the check box to the left of each rule that you want to enable, disable, or delete, or click the **Select All** table button to select all rules.
2. Click one of the following table buttons:
   - **Enable**. Enables the rule or rules. The ! status icon changes from a gray circle to a green circle, indicating that the selected rule or rules are enabled. (By default, when a rule is added to the table, it is automatically enabled.)
   - **Disable**. Disables the rule or rules. The ! status icon changes from a green circle to a gray circle, indicating that the selected rule or rules are disabled.
   - **Delete**. Deletes the selected rule or rules.

LAN WAN Outbound Service Rules

You can define rules that specify exceptions to the default rules. By adding custom rules, you can block or allow access based on the service or application, source or destination IP addresses, and time of day. An outbound rule can block or allow traffic between an internal IP LAN address and any external WAN IP address according to the schedule created in the Schedule screen.

You can also tailor these rules to your specific needs (see *Administrator Tips* on page 108).

Note: This feature is for advanced administrators. Incorrect configuration might cause serious problems.

➢ **To create a new outbound LAN WAN service rule:**

1. In the LAN WAN Rules screen, click the **Add** table button under the Outbound Services table. The Add LAN WAN Outbound Service screen displays:

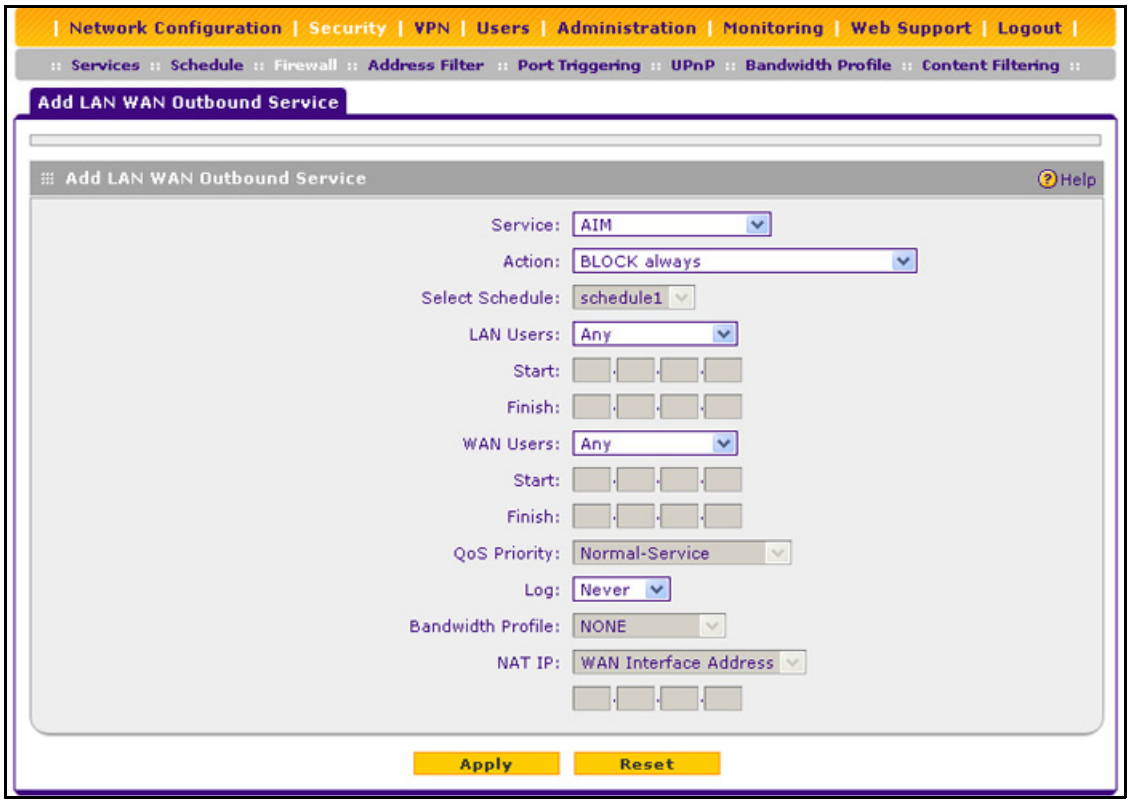

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
Add LAN WAN Outbound Service
Add LAN WAN Outbound Service
Help
Service: AIM
Action: BLOCK always
Select Schedule: schedule1
LAN Users: Any
Start:
Finish:
WAN Users: Any
Start:
Finish:
QoS Priority: Normal-Service
Log: Never
Bandwidth Profile: NONE
NAT IP: WAN Interface Address
Apply
Reset

Figure 55.

2. Enter the settings as explained in *Table 27* on page 110.
3. Click **Apply** to save your changes. The new rule is now added to the Outbound Services table.

LAN WAN Inbound Service Rules

The Inbound Services table lists all existing rules for inbound traffic. If you have not defined any rules, no rules are listed. By default, all inbound traffic (from the Internet to the LAN) is blocked. Remember that allowing inbound services opens potential security holes in your firewall. Enable only those ports that are necessary for your network.

➢ **To create a new inbound LAN WAN service rule:**

1. In the LAN WAN Rules screen, click the **Add** table button under the Inbound Services table. The Add LAN WAN Inbound Service screen displays:

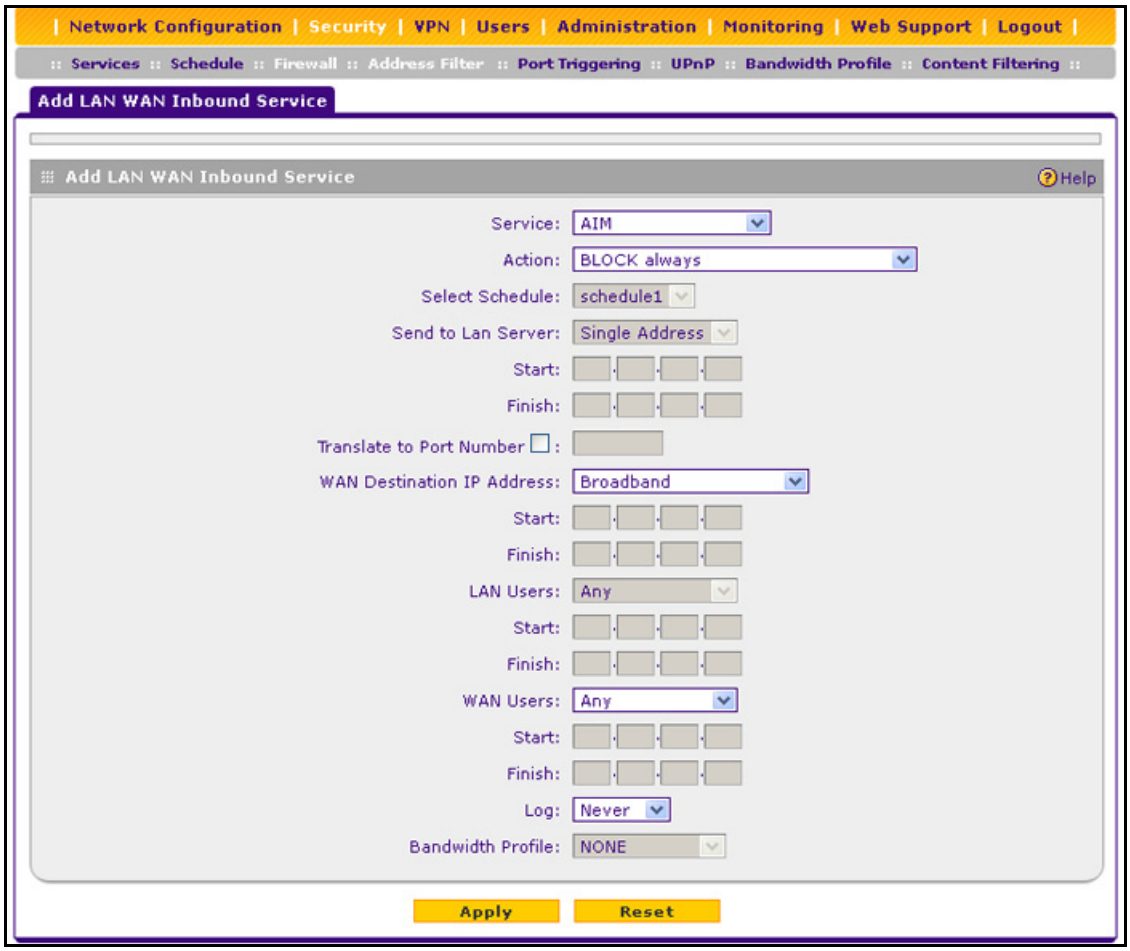


Figure 56.

2. Enter the settings as explained in *Table 28* on page 113.
3. Click **Apply** to save your changes. The new rule is now added to the Inbound Services table.

Create DMZ WAN Rules

The firewall rules for traffic between the DMZ and the Internet are configured on the DMZ WAN Rules screen. The default outbound policy is to block all traffic from and to the Internet. You can then apply firewall rules to allow specific types of traffic either going out from the DMZ to the Internet (outbound) or coming in from the Internet to the DMZ (inbound).

There is no drop-down list that lets you set the default outbound policy as there is on the LAN WAN Rules screen. You can change the default outbound policy by enabling all outbound traffic and then blocking only specific services from passing through the wireless VPN firewall. You do so by adding outbound services rules (see *DMZ WAN Outbound Service Rules* on page 121).

To access the DMZ WAN Rules screen, select **Security > Firewall > DMZ WAN Rules**. The DMZ WAN Rules screen displays. (The following figure shows a rule in the Outbound Services table as an example.)

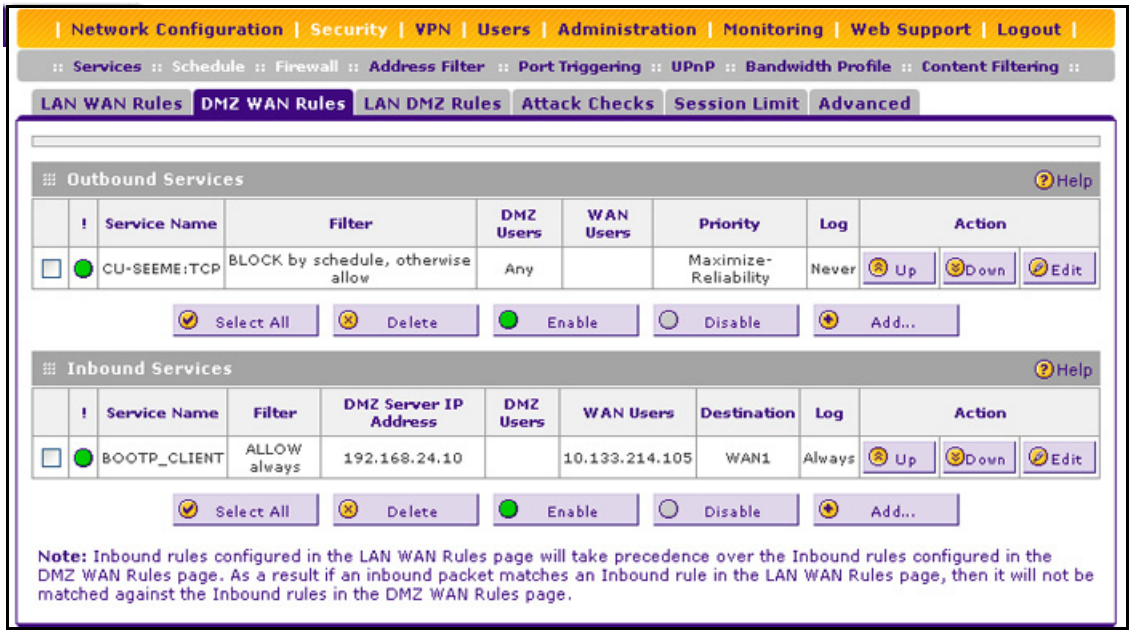

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering
LAN WAN Rules
DMZ WAN Rules
LAN DMZ Rules
Attack Checks
Session Limit
Advanced
Outbound Services
Help
! Service Name Filter DMZ Users WAN Users Priority Log Action
CU-SEEME:TCP BLOCK by schedule, otherwise allow Any Maximize-Reliability Never Up Down Edit
Select All Delete Enable Disable Add...
Inbound Services
Help
! Service Name Filter DMZ Server IP Address DMZ Users WAN Users Destination Log Action
BOOTP_CLIENT ALLOW always 192.168.24.10 10.133.214.105 WAN1 Always Up Down Edit
Select All Delete Enable Disable Add...
Note: Inbound rules configured in the LAN WAN Rules page will take precedence over the Inbound rules configured in the DMZ WAN Rules page. As a result if an inbound packet matches an Inbound rule in the LAN WAN Rules page, then it will not be matched against the Inbound rules in the DMZ WAN Rules page.

Figure 57.

➢ **To make changes to an existing outbound or inbound service rule:**

In the Action column to the right of to the rule, click one of the following table buttons:

- **Up**. Moves the rule up one position in the table rank.
- **Down**. Moves the rule down one position in the table rank.
- **Edit**. Allows you to make any changes to the definition of an existing rule. Depending on your selection, either the Edit DMZ WAN Outbound Service screen (identical to *Figure 58* on page 121) or the Edit DMZ WAN Inbound Service screen (identical to *Figure 59* on page 122) displays, containing the data for the selected rule.

➢ **To enable, disable, or delete one or more rules:**

1. select the check box to the left of each rule that you want to enable, disable, or delete, or click the **Select All** table button to select all rules.
2. Click one of the following table buttons:
   - **Enable**. Enables the rule or rules. The ! status icon changes from a gray circle to a green circle, indicating that the selected rule or rules are enabled. (By default, when a rule is added to the table, it is automatically enabled.)
   - **Disable**. Disables the rule or rules. The ! status icon changes from a green circle to a gray circle, indicating that the selected rule or rules are disabled.
   - **Delete**. Deletes the selected rule or rules.

DMZ WAN Outbound Service Rules

You can change the default outbound policy or define rules that specify exceptions to the default outbound policy. By adding custom rules, you can block or allow access based on the service or application, source or destination IP addresses, and time of day. An outbound rule can block or allow traffic between the DMZ and any external WAN IP address according to the schedule created in the Schedule screen.

➢ **To create a new outbound DMZ WAN service rule:**

1. In the DMZ WAN Rules screen, click the **Add** table button under the Outbound Services table. The Add DMZ WAN Outbound Service screen displays:

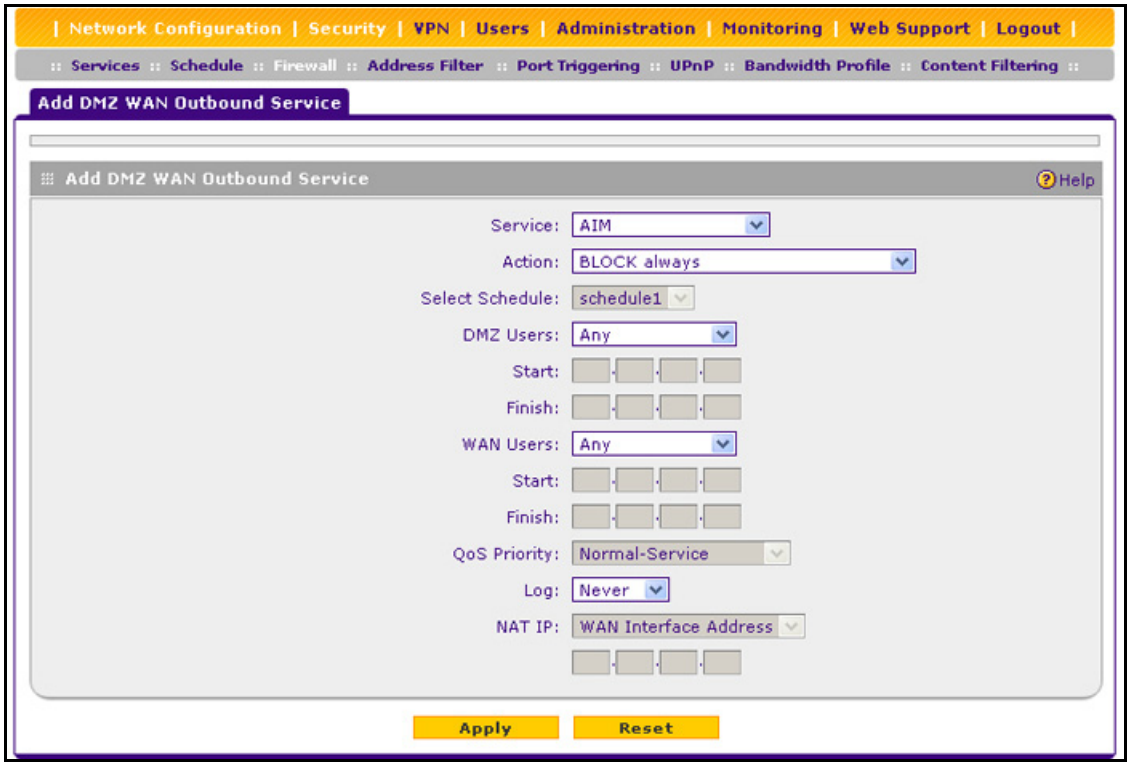

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering
Add DMZ WAN Outbound Service
Add DMZ WAN Outbound Service
Help
Service: AIM
Action: BLOCK always
Select Schedule: schedule1
DMZ Users: Any
Start:
Finish:
WAN Users: Any
Start:
Finish:
QoS Priority: Normal-Service
Log: Never
NAT IP: WAN Interface Address
Apply
Reset

Figure 58.

2. Enter the settings as explained in *Table 27* on page 110.
3. Click **Apply.** The new rule is now added to the Outbound Services table. The rule is automatically enabled.

DMZ WAN Inbound Service Rules

The Inbound Services table lists all existing rules for inbound traffic. If you have not defined any rules, no rules are listed. By default, all inbound traffic (from the Internet to the DMZ) is blocked.

Inbound rules that are configured on the LAN WAN Rules screen take precedence over inbound rules that are configured on the DMZ WAN Rules screen. As a result, if an inbound

packet matches an inbound rule on the LAN WAN Rules screen, it is not matched against the inbound rules on the DMZ WAN Rules screen.

➢ **To create a new inbound DMZ WAN service rule:**

1. In the DMZ WAN Rules screen, click the **Add** table button under the Inbound Services table. The Add DMZ WAN Inbound Service screen displays:

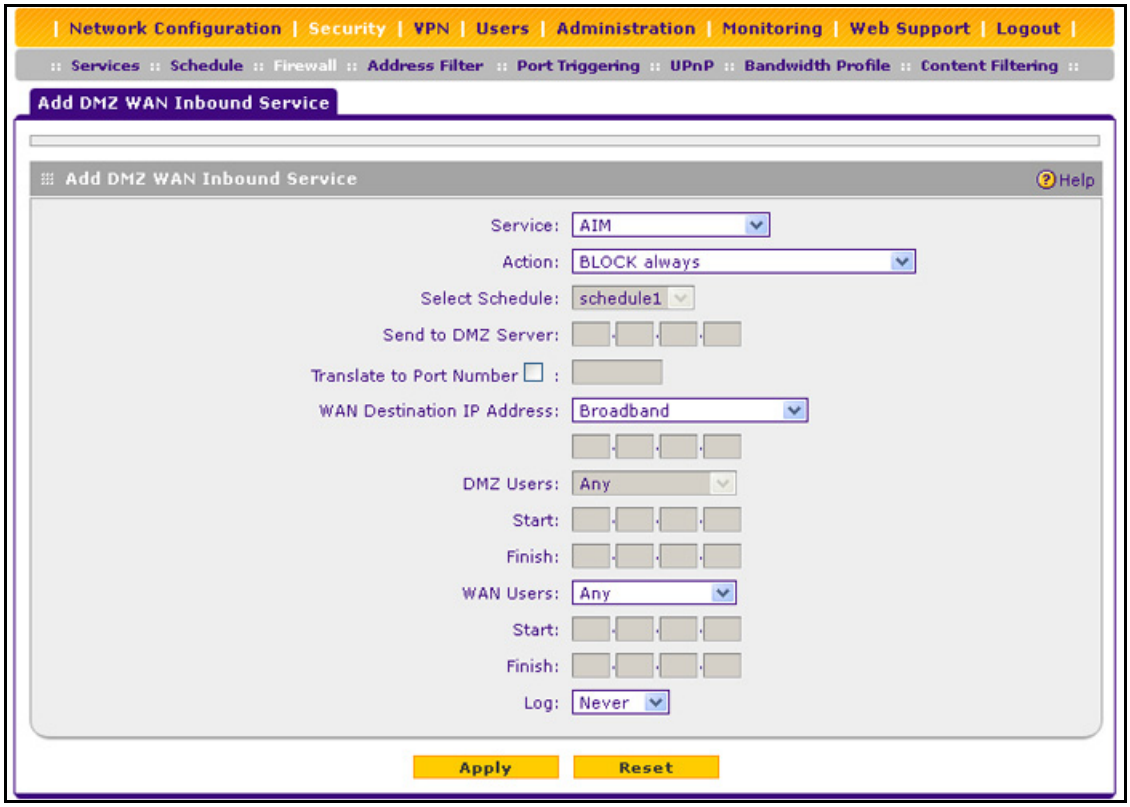

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering
Add DMZ WAN Inbound Service
Add DMZ WAN Inbound Service
Help
Service: AIM
Action: BLOCK always
Select Schedule: schedule1
Send to DMZ Server:
Translate to Port Number :
WAN Destination IP Address: Broadband
DMZ Users: Any
Start:
Finish:
WAN Users: Any
Start:
Finish:
Log: Never
Apply
Reset

Figure 59.

2. Enter the settings as explained in *Table 28* on page 113.
3. Click **Apply** to save your changes. The new rule is now added to the Inbound Services table.

Create LAN DMZ Rules

The LAN DMZ Rules screen allows you to create rules that define the movement of traffic between the LAN and the DMZ. The default outbound and inbound policies are to block all traffic between the local LAN and DMZ network. You can then apply firewall rules to allow specific types of traffic either going out from the LAN to the DMZ (outbound) or coming in from the DMZ to the LAN (inbound).

There is no drop-down list that lets you set the default outbound policy as there is on the LAN WAN Rules screen. You can change the default outbound policy by allowing all outbound traffic and then blocking specific services from passing through the wireless VPN firewall. You

do so by adding outbound service rules (see *LAN DMZ Outbound Service Rules* on page 124).

To access the LAN DMZ Rules screen and to make changes to an existing outbound or inbound service rule, select **Security > Firewall > LAN DMZ Rules**. The LAN DMZ Rules screen displays:

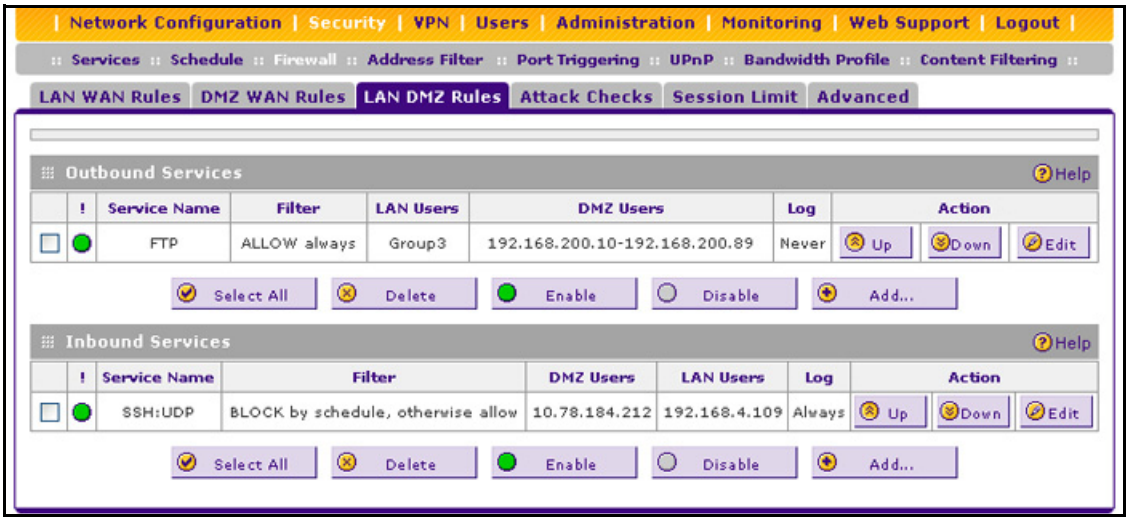

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering
LAN WAN Rules
DMZ WAN Rules
LAN DMZ Rules
Attack Checks
Session Limit
Advanced
Outbound Services
Help
! Service Name Filter LAN Users DMZ Users Log Action
FTP ALLOW always Group3 192.168.200.10-192.168.200.89 Never Up Down Edit
Select All Delete Enable Disable Add...
Inbound Services
Help
! Service Name Filter DMZ Users LAN Users Log Action
SSH:UDP BLOCK by schedule, otherwise allow 10.78.184.212 192.168.4.109 Always Up Down Edit
Select All Delete Enable Disable Add...

Figure 60.

In the Action column to the right of to the rule, click one of the following table buttons:

- **Up**. Moves the rule up one position in the table rank.
- **Down**. Moves the rule down one position in the table rank.
- **Edit**. Allows you to make any changes to the rule definition of an existing rule. Depending on your selection, either the Edit LAN DMZ Outbound Service screen (identical to *Figure 61* on page 124) or the Edit LAN DMZ Inbound Service screen (identical to *Figure 62* on page 125) displays, containing the data for the selected rule.

➢ **To enable, disable, or delete one or more rules:**

1. Select the check box to the left of each rule that you want to enable, disable, or delete, or click the **Select All** table button to select all rules.
2. Click one of the following table buttons:
   - **Enable**. Enables the rule or rules. The ! status icon changes from a gray circle to a green circle, indicating that the selected rule or rules are enabled. (By default, when a rule is added to the table, it is automatically enabled.)
   - **Disable**. Disables the rule or rules. The ! status icon changes from a green circle to a gray circle, indicating that the selected rule or rules are disabled.
   - **Delete**. Deletes the selected rule or rules.

LAN DMZ Outbound Service Rules

You can change the default outbound policy or define rules that specify exceptions to the default outbound policy. By adding custom rules, you can block or allow access based on the service or application, source or destination IP addresses, and time of day. An outbound rule can block or allow traffic between the DMZ and any internal LAN IP address according to the schedule created in the Schedule screen.

➤ **To create a new outbound LAN DMZ service rule:**

1. In the LAN DMZ Rules screen, click the **Add** table button under the Outbound Services table. The Add LAN DMZ Outbound Service screen displays:

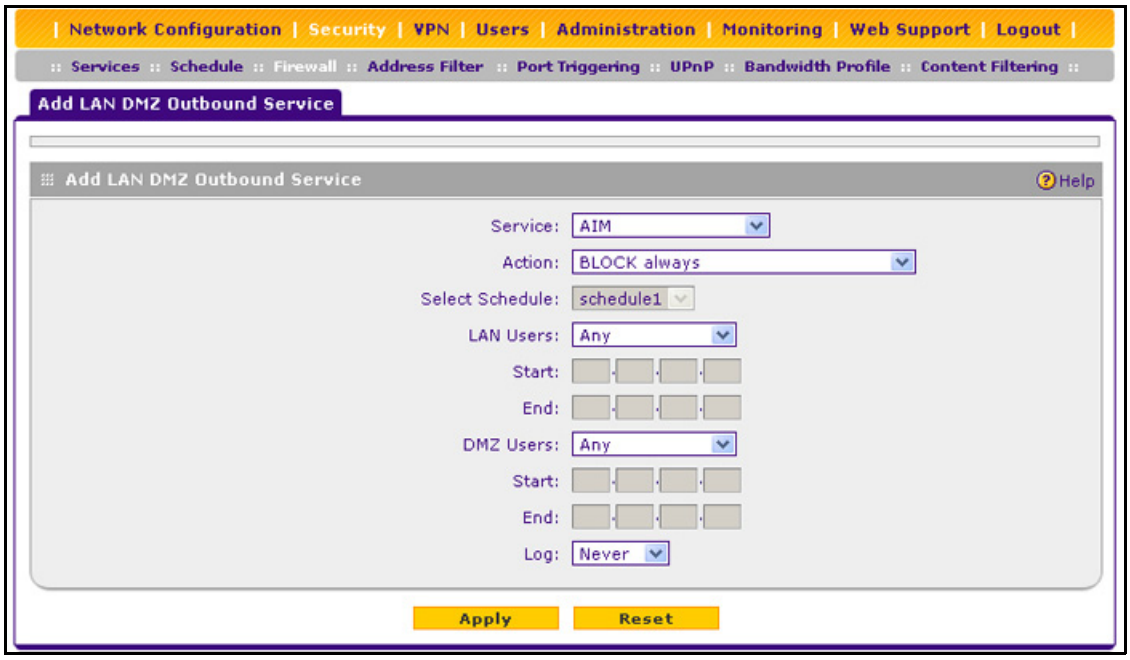

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering
Add LAN DMZ Outbound Service
Add LAN DMZ Outbound Service
Help
Service: AIM
Action: BLOCK always
Select Schedule: schedule1
LAN Users: Any
Start:
End:
DMZ Users: Any
Start:
End:
Log: Never
Apply
Reset

Figure 61.

2. Enter the settings as explained in *Table 27* on page 110.
3. Click **Apply.** The new rule is now added to the Outbound Services table. The rule is automatically enabled.

LAN DMZ Inbound Service Rules

The Inbound Services table lists all existing rules for inbound traffic. If you have not defined any rules, no rules are listed. By default, all inbound traffic (from the LAN to the DMZ) is blocked.

➢ **To create a new inbound LAN DMZ service rule:**

1. In the LAN DMZ Rules screen, click the **Add** table button under the Inbound Services table. The Add LAN DMZ Inbound Service screen displays:

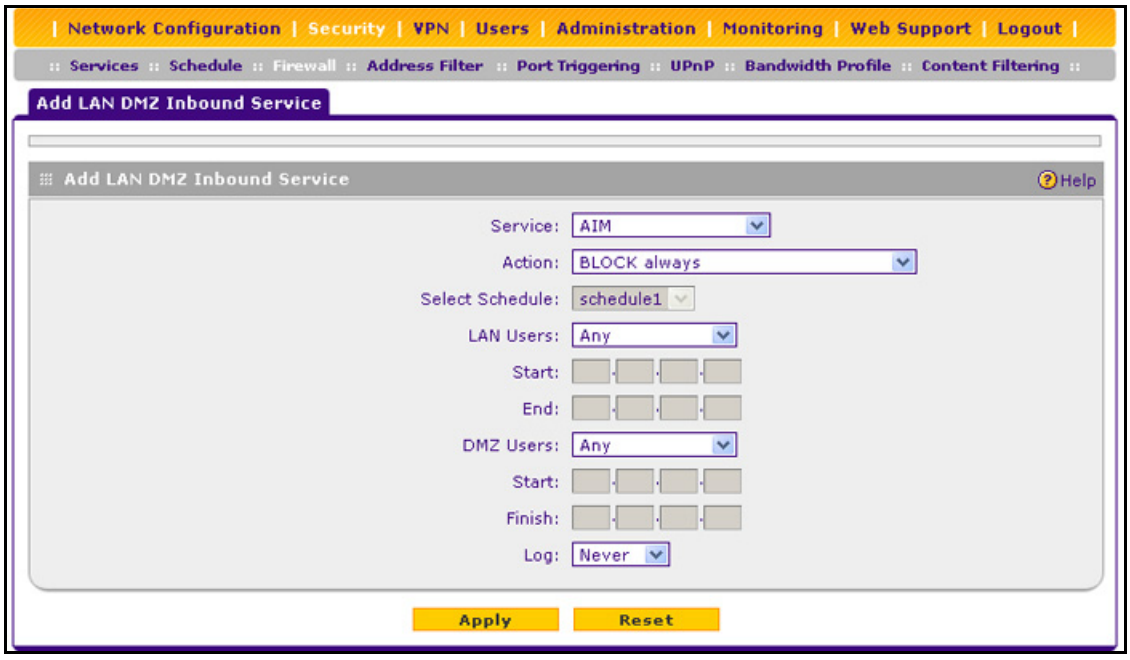

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering
Add LAN DMZ Inbound Service
Add LAN DMZ Inbound Service
Help
Service: AIM
Action: BLOCK always
Select Schedule: schedule1
LAN Users: Any
Start:
End:
DMZ Users: Any
Start:
Finish:
Log: Never
Apply
Reset

Figure 62.

2. Enter the settings as explained in *Table 28* on page 113.
3. Click **Apply** to save your changes. The new rule is now added to the Inbound Services table.

Inbound Rule Examples

LAN WAN Inbound Rule: Host a Local Public Web Server

If you host a public web server on your local network, you can define a rule to allow inbound web (HTTP) requests from any outside IP address to the IP address of your web server at any time of the day.

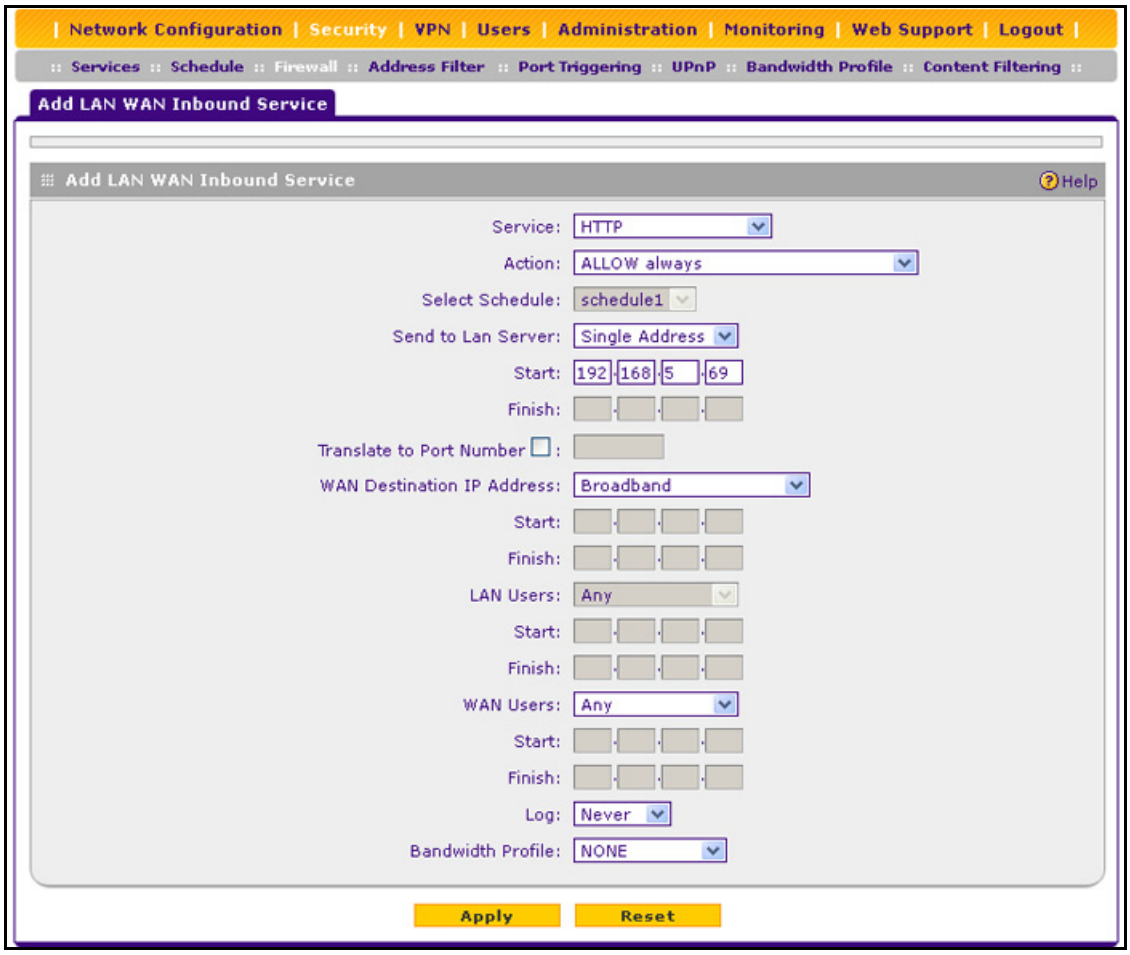


Figure 63.

LAN WAN Inbound Rule: Allow Videoconference from Restricted Addresses

If you want to allow incoming videoconferencing to be initiated from a restricted range of outside IP addresses, such as from a branch office, you can create an inbound rule (see the following figure). In the example, CU-SeeMe connections are allowed only from a specified range of external IP addresses.

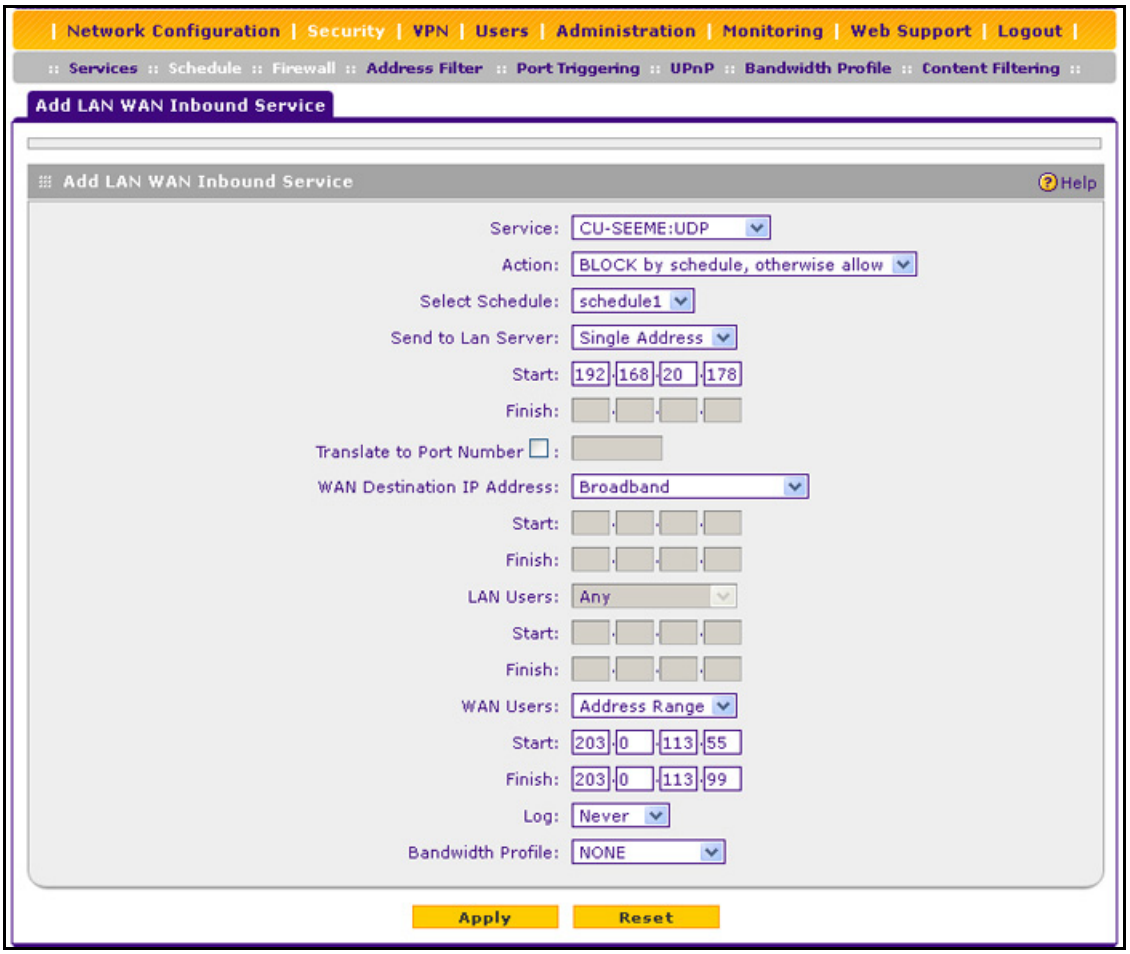


Figure 64.

LAN WAN or DMZ WAN Inbound Rule: Set Up One-to-One NAT Mapping

In this example, multi-NAT is configured to support multiple public IP addresses on one WAN interface. An inbound rule configures the wireless VPN firewall to host an additional public IP address and associate this address with a web server on the LAN.

The following addressing scheme is used to illustrate this procedure:

- NETGEAR wireless VPN firewall:
  - WAN IP address. 10.1.0.118
  - LAN IP address subnet. 192.168.1.1 with subnet 255.255.255.0
  - DMZ IP address subnet. 192.168.10.1 with subnet 255.255.255.0
- Web server PC on the wireless VPN firewall's LAN:
  - LAN IP address. 192.168.1.2
  - DMZ IP address. 192.168.10.2
  - Access to web server is (simulated) public IP address. 10.1.0.52

Tip: If you arrange with your ISP to have more than one public IP address for your use, you can use the additional public IP addresses to map to servers on your LAN or DMZ. One of these public IP addresses is used as the primary IP address of the router that provides Internet access to your LAN PCs through NAT. The other addresses are available to map to your servers.

➢ **To configure the wireless VPN firewall for additional IP addresses:**

1. Select **Security > Firewall**. The Firewall submenu tabs display.
2. If your server is to be on your LAN, click the **LAN WAN Rules** submenu tab. (This is the screen used in this example). If your server is to be on your DMZ, click the **DMZ WAN Rules** submenu tab.
3. Click the **Add** table button under the Inbound Services table. The Add LAN WAN Inbound Service screen displays:

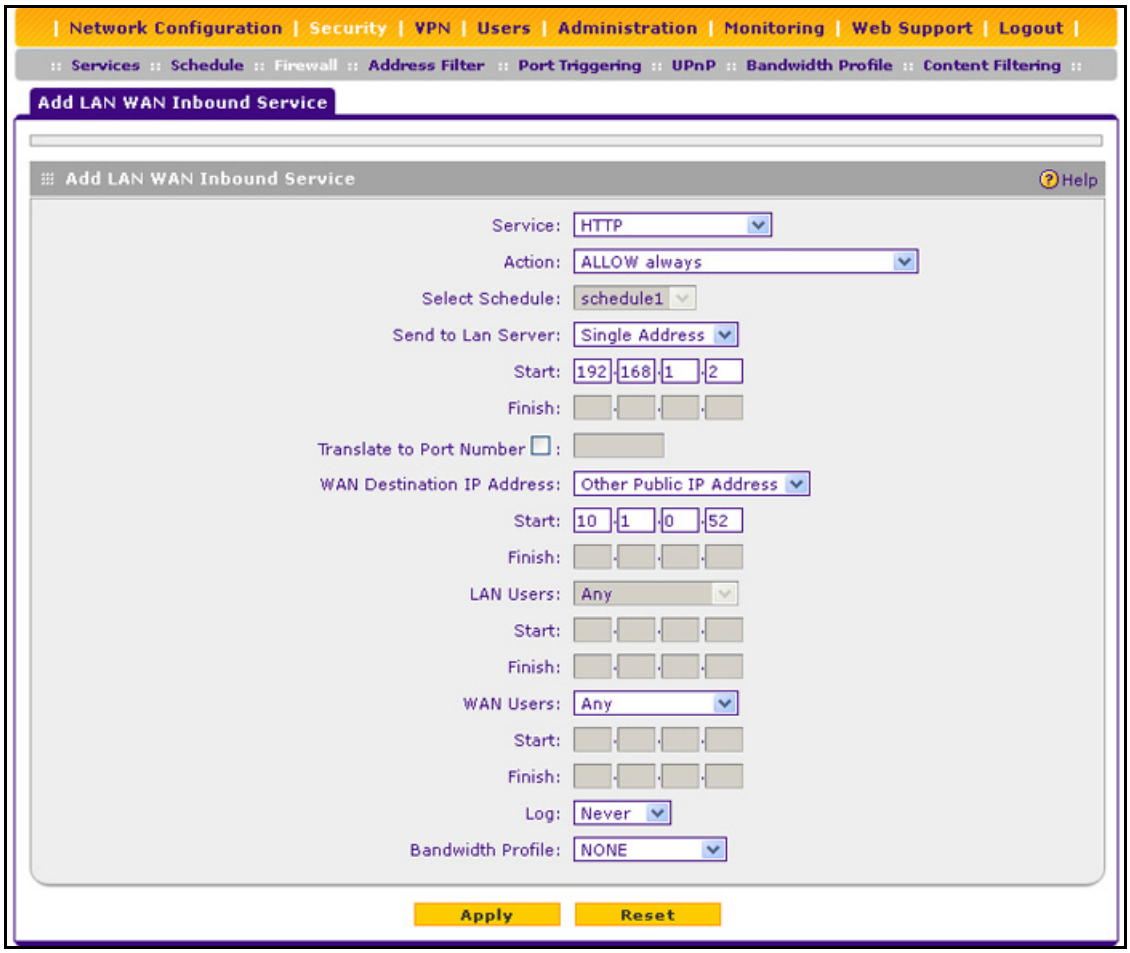

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering
Add LAN WAN Inbound Service
Add LAN WAN Inbound Service
Help
Service: HTTP
Action: ALLOW always
Select Schedule: schedule1
Send to Lan Server: Single Address
Start: 192 168 1 2
Finish:
Translate to Port Number:
WAN Destination IP Address: Other Public IP Address
Start: 10 1 0 52
Finish:
LAN Users: Any
Start:
Finish:
WAN Users: Any
Start:
Finish:
Log: Never
Bandwidth Profile: NONE
Apply
Reset

Figure 65.

4. From the Service drop-down list, select **HTTP** for a web server.
5. From the Action drop-down list, select **ALLOW Always**.
6. In the Send to LAN Server field, enter the local IP address of your web server PC (192.168.1.2 in this example).
7. In the WAN Destination IP Address fields, enter **10.1.0.52**.
8. Click **Apply** to save your settings. The rule is now added to the Inbound Services table of the LAN WAN Rules screen.

To test the connection from a PC on the Internet, type **http://*<IP_address>***, in which <*IP_address*> is the public IP address that you have mapped to your web server in *step 7*. You should see the home page of your web server.

LAN WAN or DMZ WAN Inbound Rule: Specifying an Exposed Host

Specifying an exposed host allows you to set up a computer or server that is available to anyone on the Internet for services that you have not yet defined.

WARNING!

Do not set up an exposed host from a remote connection because you will very likely lock yourself out from the wireless VPN firewall.

➢ **To expose one of the PCs on your LAN or DMZ as this host:**

1. Create an inbound rule that allows all protocols.
2. Place the rule below all other inbound rules.

See an example in the following figure. (The inbound rule that allows all protocols is disabled in this figure.)

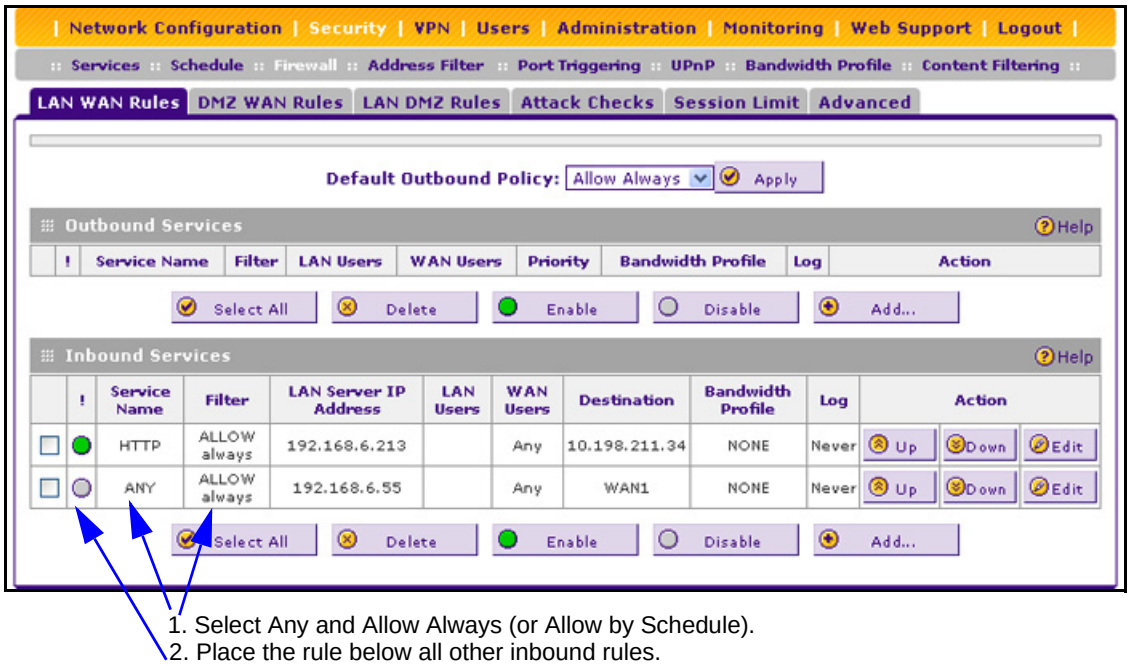

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering
LAN WAN Rules
DMZ WAN Rules
LAN DMZ Rules
Attack Checks
Session Limit
Advanced
Default Outbound Policy: Allow Always
Apply
Outbound Services
Help
! Service Name Filter LAN Users WAN Users Priority Bandwidth Profile Log Action
Select All
Delete
Enable
Disable
Add...
Inbound Services
Help
! Service Name Filter LAN Server IP Address LAN Users WAN Users Destination Bandwidth Profile Log Action
HTTP ALLOW always 192.168.6.213 Any 10.198.211.34 NONE Never Up Down Edit
ANY ALLOW always 192.168.6.55 Any WAN1 NONE Never Up Down Edit
Select All
Delete
Enable
Disable
Add...
1. Select Any and Allow Always (or Allow by Schedule).
2. Place the rule below all other inbound rules.

Figure 66.

WARNING!

For security, NETGEAR strongly recommends that you avoid creating an exposed host. When a computer is designated as the exposed host, it loses much of the protection of the firewall and is exposed to many exploits from the Internet. If compromised, the computer can be used to attack your network.

Outbound Rule Example

Outbound rules let you prevent users from using applications such as Instant Messenger, Real Audio, or other nonessential sites.

LAN WAN Outbound Rule: Block Instant Messenger

If you want to block Instant Messenger usage by employees during working hours, you can create an outbound rule to block such an application from any internal IP address to any external address according to the schedule that you have created in the Schedule screen. See an example in the following figure.

You can also enable the wireless VPN firewall to log any attempt to use Instant Messenger during the blocked period.

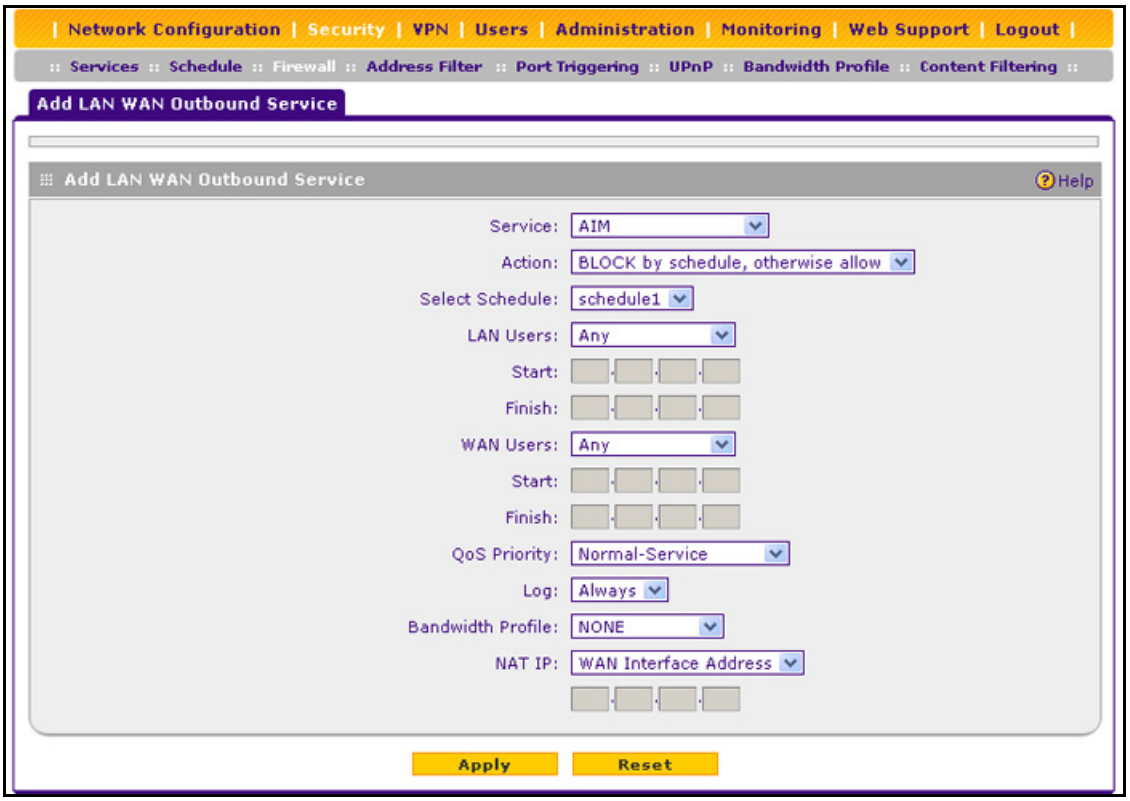

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering
Add LAN WAN Outbound Service
Add LAN WAN Outbound Service
Help
Service: AIM
Action: BLOCK by schedule, otherwise allow
Select Schedule: schedule1
LAN Users: Any
Start:
Finish:
WAN Users: Any
Start:
Finish:
QoS Priority: Normal-Service
Log: Always
Bandwidth Profile: NONE
NAT IP: WAN Interface Address
Apply
Reset

Figure 67.

Configure Other Firewall Features

You can configure attack checks, set session limits, and manage the application level gateway (ALG) for SIP sessions.

Attack Checks

The Attack Checks screen allows you to specify whether or not the wireless VPN firewall should be protected against common attacks in the DMZ, LAN, and WAN networks. The various types of attack checks are listed on the Attack Checks screen and defined in *Table 29* on page 132.

➢ **To enable the appropriate attack checks for your network environment:**

1. Select **Security > Firewall > Attack Checks**. The Attack Checks screen displays:

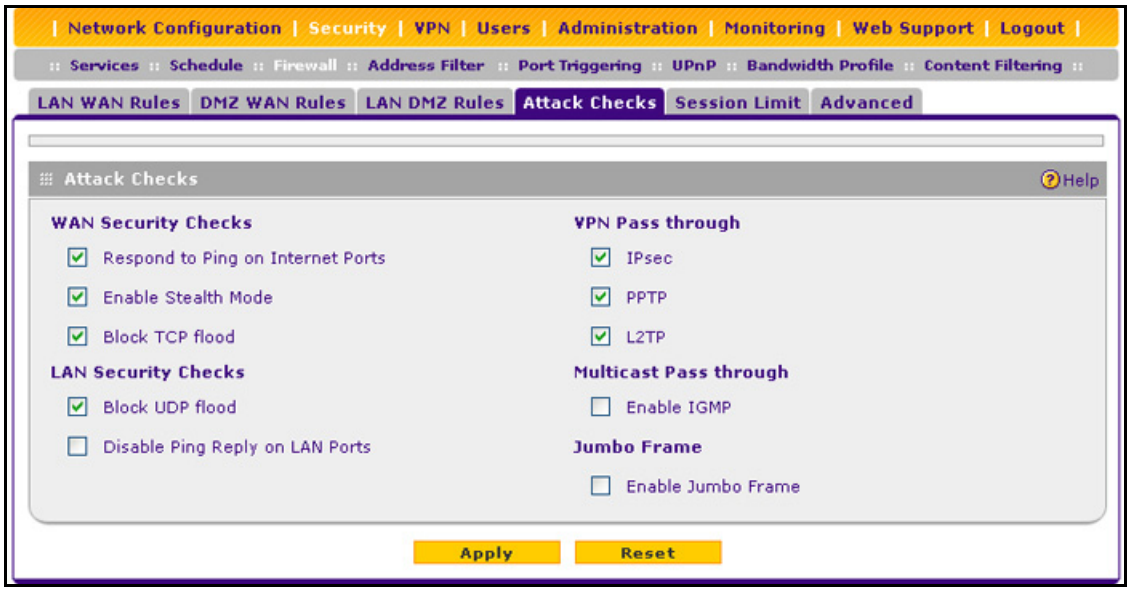


Figure 68.

2. Enter the settings as explained in the following table:

Table 29. Attack Checks screen settings

Setting	Description
WAN Security Checks	
Respond to Ping on Internet Ports	Select the **Respond to Ping on Internet Ports** check box to enable the wireless VPN firewall to respond to a ping from the Internet. A ping can be used as a diagnostic tool. Keep this check box cleared unless you have a specific reason to enable the wireless VPN firewall to respond to a ping from the Internet.

Table 29. Attack Checks screen settings (continued)

Setting	Description
Enable Stealth Mode	Select the **Enable Stealth Mode** check box (which is the default setting) to prevent the wireless VPN firewall from responding to port scans from the WAN, thus making it less susceptible to discovery and attacks.
Block TCP flood	Select the **Block TCP flood** check box to enable the wireless VPN firewall to drop all invalid TCP packets and to protect the wireless VPN firewall from a SYN flood attack. A SYN flood is a form of denial of service attack in which an attacker sends a succession of SYN (synchronize) requests to a target system. When the system responds, the attacker does not complete the connections, thus leaving the connection half open and flooding the server with SYN messages. No legitimate connections can then be made. By default, the Block TCP flood check box is cleared.
LAN Security Checks	
Block UDP flood	Select the **Block UDP flood** check box to prevent the wireless VPN firewall from accepting more than 20 simultaneous, active User Datagram Protocol (UDP) connections from a single device on the LAN. By default, the Block UDP flood check box is cleared. A UDP flood is a form of denial of service attack that can be initiated when one device sends a large number of UDP packets to random ports on a remote host. As a result, the distant host does the following: 1. Checks for the application listening at that port. 2. Sees that no application is listening at that port. 3. Replies with an ICMP Destination Unreachable packet. When the victimized system is flooded, it is forced to send many ICMP packets, eventually making it unreachable by other clients. The attacker might also spoof the IP address of the UDP packets, ensuring that the excessive ICMP return packets do not reach the attacker, thus making the attacker's network location anonymous.
Disable Ping Reply on LAN Ports	Select the **Disable Ping Reply on LAN Ports** check box to prevent the wireless VPN firewall from responding to a ping on a LAN port. A ping can be used as a diagnostic tool. Keep this check box cleared unless you have a specific reason to prevent the wireless VPN firewall from responding to a ping on a LAN port.
VPN Pass through	
IPSec PPTP L2TP	When the wireless VPN firewall functions in NAT mode, all packets going to the remote VPN gateway are first filtered through NAT and then encrypted according to the VPN policy. For example, if a VPN client or gateway on the LAN side of the wireless VPN firewall wants to connect to another VPN endpoint on the WAN side (placing the wireless VPN firewall between two VPN endpoints), encrypted packets are sent to the wireless VPN firewall. Because the wireless VPN firewall filters the encrypted packets through NAT, the packets become invalid unless you enable the VPN Pass through feature. To enable the VPN tunnel to pass the VPN traffic without any filtering, select any or all of the following check boxes: • **IPSec**. Disables NAT filtering for IPSec tunnels. • **PPTP**. Disables NAT filtering for PPTP tunnels. • **L2TP**. Disables NAT filtering for L2TP tunnels. By default, all three check boxes are selected.

Table 29. Attack Checks screen settings (continued)

Setting	Description
Multicast Pass through	
Enable IGMP	IP multicast pass-through allows multicast packets that originate in the WAN subnet, such as packets from a media streaming or gaming application, to be forwarded to the LAN subnet. Internet Group Management Protocol (IGMP) is used to support multicast between IP hosts and their adjacent neighbors. Select the **Enable IGMP** check box to enable IP multicast pass-through. By default, IP multicast pass-through is disabled.
Jumbo Frames	
Enable Jumbo Frame	Jumbo frames allow multiple smaller packets to be combined into a single larger packet, reducing network overhead and increasing data transfer performance. Select the **Jumbo Frame** check box to enable jumbo frames. By default, jumbo frames are disabled. **Note:** Jumbo frames are not supported on Fast Ethernet interfaces.

3. Click **Apply** to save your settings.

Set Session Limits

The session limits feature allows you to specify the total number of sessions that are allowed, per user, over an IP connection across the wireless VPN firewall. The session limits feature is disabled by default.

➢ **To enable and configure session limits:**

1. Select **Security > Firewall > Session Limit**. The Session Limit screen displays:

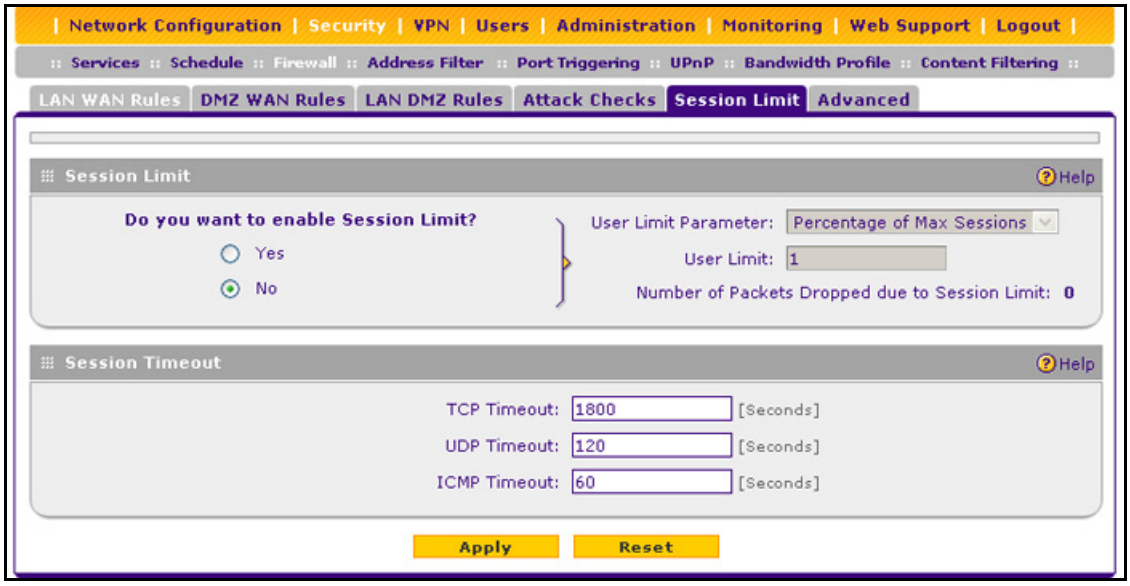


Figure 69.

2. Select the **Yes** radio button under Do you want to enable Session Limit?
3. Enter the settings as explained in the following table:

Table 30. Session Limit screen settings

Setting	Description
Session Limit	
User Limit Parameter	From the User Limit Parameter drop-down list, select one of the following options: • **Percentage of Max Sessions**. A percentage of the total session connection capacity of the wireless VPN firewall. • **Number of Sessions**. An absolute number of maximum sessions.
User Limit	Enter a number to indicate the user limit. Note the following: • If the User Limit Parameter is set to Percentage of Max Sessions, the number specifies the maximum number of sessions that are allowed from a single-source device as a percentage of the total session connection capacity of the wireless VPN firewall. (The session limit is per-device based.) • If the User Limit Parameter is set to Number of Sessions, the number specifies an absolute value. **Note:** Some protocols such as FTP and RSTP create two sessions per connection, which should be considered when configuring a session limit.
Total Number of Packets Dropped due to Session Limit	This is a nonconfigurable counter that displays the total number of dropped packets when the session limit is reached.
Session Timeout	
TCP Timeout	For each protocol, specify a time-out in seconds. A session expires if no data for the session is received for the duration of the time-out period. The default time-out periods are 1800 seconds for TCP sessions, 120 seconds for UDP sessions, and 60 seconds for ICMP sessions.
UDP Timeout	
ICMP Timeout	

4. Click **Apply** to save your settings.

Manage the Application Level Gateway for SIP Sessions

The application level gateway (ALG) facilitates multimedia sessions such as voice over IP (VoIP) sessions that use the Session Initiation Protocol (SIP) across the firewall and provides support for multiple SIP clients. ALG support for SIP is disabled by default.

➢ **To enable ALG for SIP:**

1. Select **Security > Firewall > Advanced**. The Advanced screen displays:

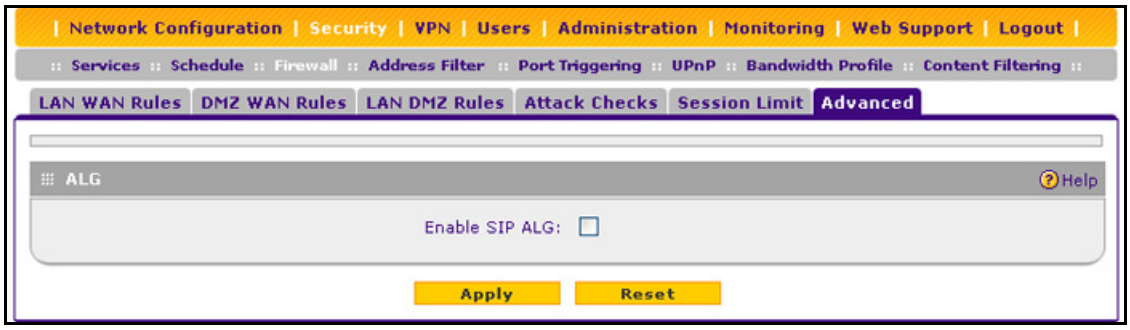


Figure 70.

2. Select the **Enable SIP ALG** check box.
3. Click **Apply** to save your settings.

Services, Bandwidth Profiles, and QoS Profiles

When you create inbound and outbound firewall rules, you use firewall objects such as services, QoS profiles, bandwidth profiles, and schedules to narrow down the firewall rules:

- **Services**. A service narrows down the firewall rule to an application and a port number. For information about adding services, see *Add Customized Services* on page 136.
- **Bandwidth profiles**. A bandwidth profile allocates and limits traffic bandwidth for the LAN users to which a firewall rule is applied. For information about creating bandwidth profiles, see *Create Bandwidth Profiles* on page 139.
- **QoS profiles**. A Quality of Service (QoS) profile defines the relative priority of an IP packet for traffic that matches the firewall rule. For information about QoS profiles, see *Preconfigured Quality of Service Profiles* on page 141.

Note: A schedule narrows down the period during which a firewall rule is applied. For information about specifying schedules, see *Set a Schedule to Block or Allow Specific Traffic* on page 146.

Add Customized Services

Services are functions performed by server computers at the request of client computers. You can configure up to 125 custom services.

For example, web servers serve web pages, time servers serve time and date information, and game hosts serve data about other players' moves. When a computer on the Internet sends a request for service to a server computer, the requested service is identified by a service or port number. This number appears as the destination port number in the transmitted IP packets. For example, a packet that is sent with destination port number 80 is an HTTP (web server) request.

The service numbers for many common protocols are defined by the Internet Engineering Task Force (IETF) and published in RFC 1700, *Assigned Numbers*. Service numbers for other applications are typically chosen from the range 1024 to 65535 by the authors of the application.

Although the wireless VPN firewall already holds a list of many service port numbers, you are not limited to these choices. Use the Services screen to add additional services and applications to the list for use in defining firewall rules. The Services screen shows a list of services that you have defined, as shown in the following figure.

To define a new service, you need to determine first which port number or range of numbers is used by the application. You can usually determine this information by contacting the publisher of the application, user groups, or newsgroups. When you have the port number information, you can enter it on the Services screen.

➢ **To add a customized service:**

1. Select **Security > Services**. The Services screen displays. The Custom Services table shows the user-defined services. (The following figure shows some examples.)

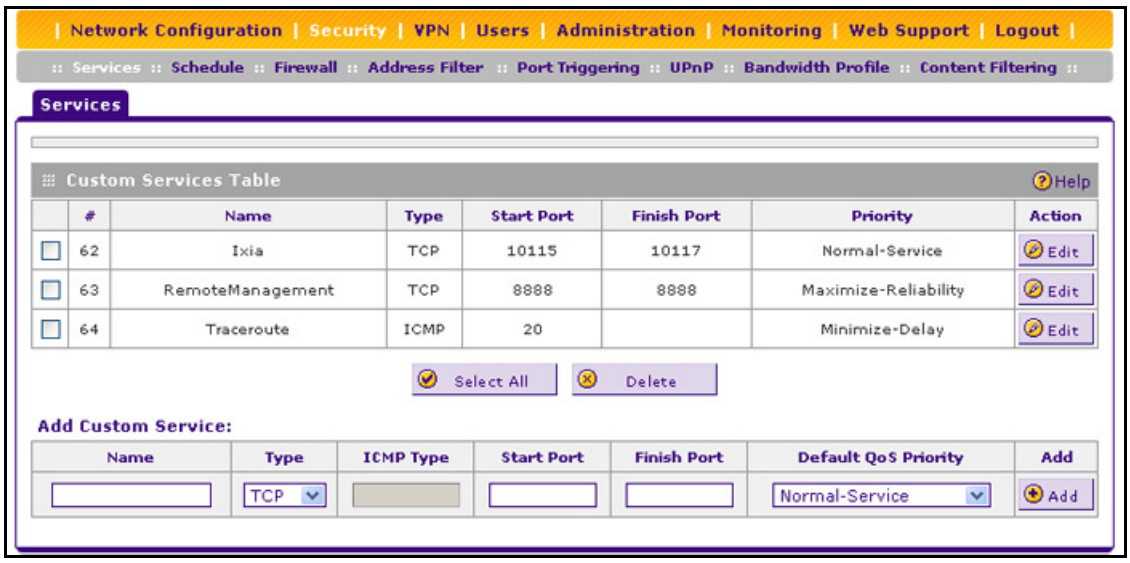

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
Services | Schedule | Firewall | Address Filter | Port Triggering | UPnP | Bandwidth Profile | Content Filtering
Services
Custom Services Table
Help
Name Type Start Port Finish Port Priority Action
62 Ixia TCP 10115 10117 Normal-Service Edit
63 RemoteManagement TCP 8888 8888 Maximize-Reliability Edit
64 Traceroute ICMP 20 Minimize-Delay Edit
Select All
Delete
Add Custom Service:
Name Type ICMP Type Start Port Finish Port Default QoS Priority Add
TCP
Normal-Service
Add

Figure 71.

2. In the Add Customer Service section of the screen, enter the settings as explained in the following table:

Table 31. Services screen settings

Setting	Description
Name	A descriptive name of the service for identification and management purposes.
Type	From the Type drop-down list, select the Layer 3 protocol that the service uses as its transport protocol: • **TCP** • **UDP** • **ICMP**

Table 31. Services screen settings (continued)

Setting	Description
ICMP Type	A numeric value that can range between 0 and 40. For a list of ICMP types, see *http://www.iana.org/assignments/icmp-parameters*. **Note:** This field is enabled only when you select ICMP from the Type drop-down list.
Start Port	The first TCP or UDP port of a range that the service uses. **Note:** This field is enabled only when you select TCP or UDP from the Type drop-down list.
Finish Port	The last TCP or UDP port of a range that the service uses. If the service uses only a single port number, enter the same number in the Start Port and Finish Port fields. **Note:** This field is enabled only when you select TCP or UDP from the Type drop-down list.
Default QoS Priority	From the Default QoS Priority drop-down list, select the QoS profile that you want to assign to the service. For more information about QoS profiles, see *Preconfigured Quality of Service Profiles* on page 141.

3. Click **Apply** to save your settings. The new custom service is added to the Custom Services table.

➢ **To edit a service:**

1. In the Custom Services table, click the **Edit** table button to the right of the service that you want to edit. The Edit Service screen displays:

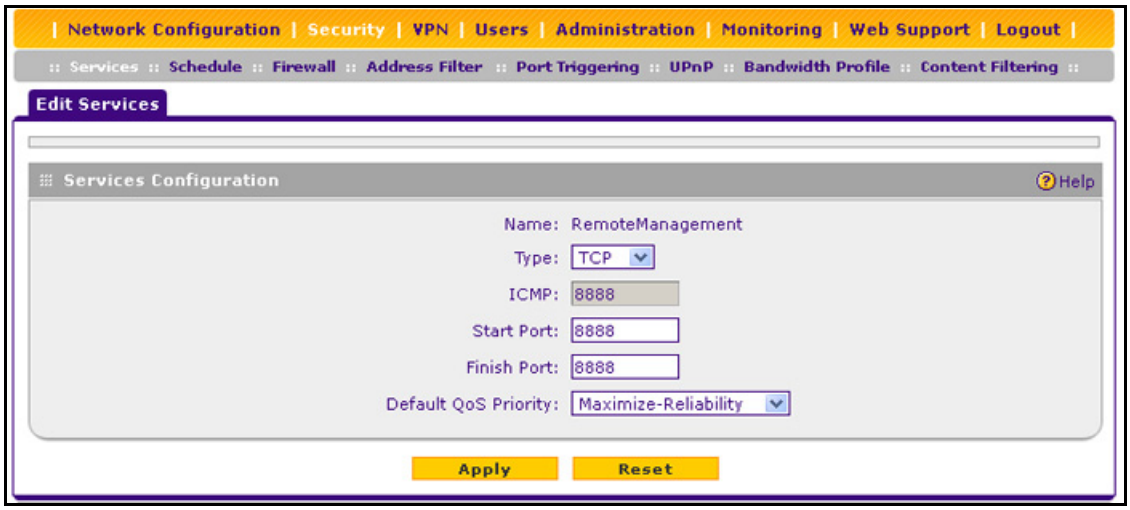

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering
Edit Services
Services Configuration
Help
Name: RemoteManagement
Type: TCP
ICMP: 8888
Start Port: 8888
Finish Port: 8888
Default QoS Priority: Maximize-Reliability
Apply
Reset

Figure 72.

2. Modify the settings that you wish to change (see the previous table).
3. Click **Apply** to save your changes. The modified service is displayed in the Custom Services table.

➢ **To delete one or more services:**

1. In the Custom Services table, select the check box to the left of each service that you want to delete, or click the **Select All** table button to select all services.
2. Click the **Delete** table button.

Create Bandwidth Profiles

Bandwidth profiles determine the way in which data is communicated with the hosts. The purpose of bandwidth profiles is to provide a method for allocating and limiting traffic, thus allocating LAN users sufficient bandwidth while preventing them from consuming all the bandwidth on your WAN link. A single bandwidth profile can be for both outbound and inbound traffic.

For outbound traffic, you can apply bandwidth profiles on the WAN interface; for inbound traffic, you can apply bandwidth profiles to a LAN interface. Bandwidth profiles do not apply to the DMZ interface.

When a new connection is established by a device, the device locates the firewall rule corresponding to the connection.

- If the rule has a bandwidth profile specification, the device creates a bandwidth class in the kernel.
- If multiple connections correspond to the same firewall rule, the connections all share the same bandwidth class.

An exception occurs for an individual bandwidth profile if the classes are per-source IP address classes. The source IP address is the IP address of the first packet that is transmitted for the connection. So for outbound firewall rules, the source IP address is the LAN-side IP address; for inbound firewall rules, the source IP address is the WAN-side IP address. The class is deleted when all the connections that are using the class expire.

After you have created a bandwidth profile, you can assign the bandwidth profile to firewall rules on the following screens:

- Add LAN WAN Outbound Services screen (see *Figure 55* on page 118).
- Add LAN WAN Inbound Services screen (see *Figure 56* on page 119).

➢ **To add and enable a bandwidth profile:**

1. Select **Security > Bandwidth Profiles**. The Bandwidth Profiles screen displays. (The following figure shows some examples.)

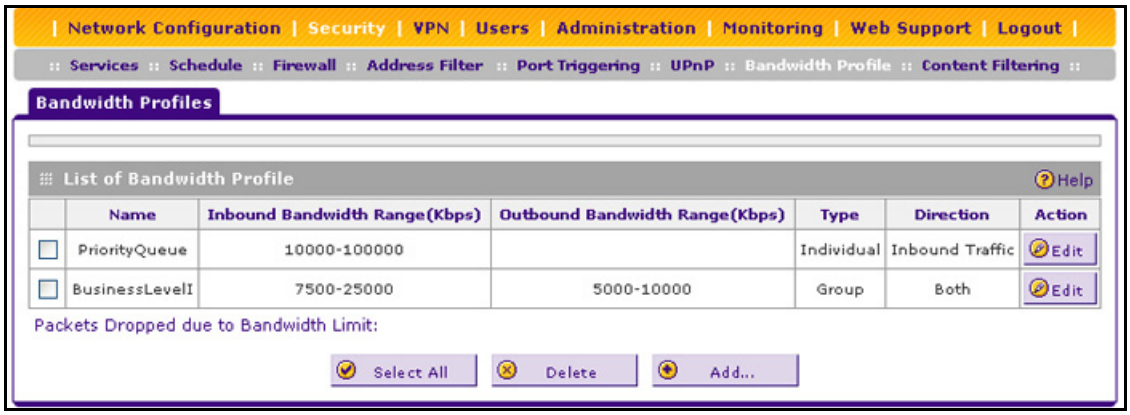


Figure 73.

2. Under the List of Bandwidth Profiles table, click the **Add** table button. The Add Bandwidth Profile screen displays:

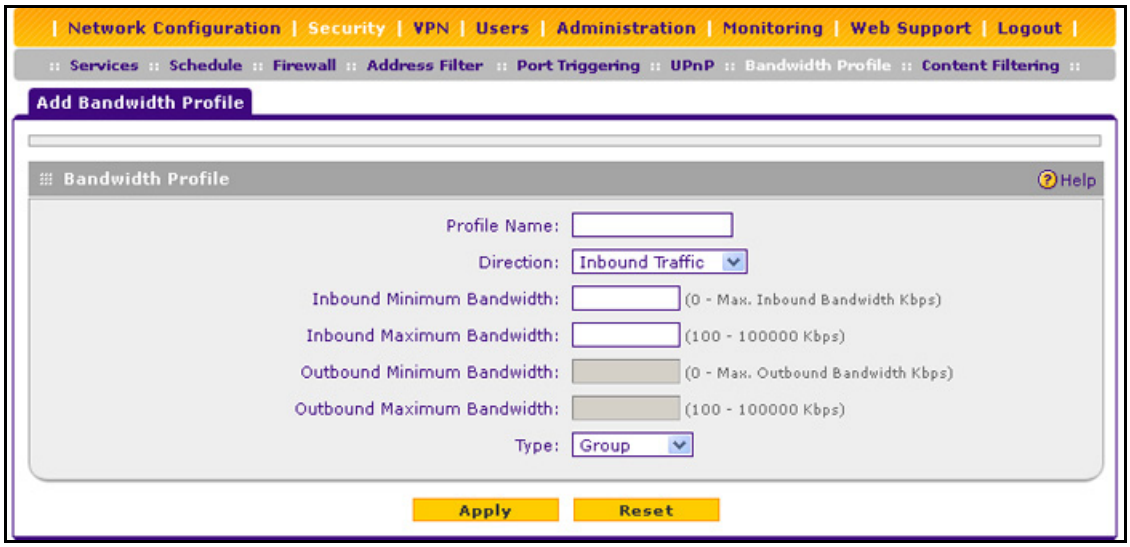

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
Add Bandwidth Profile
Bandwidth Profile
Help
Profile Name:
Direction:
Inbound Traffic
Inbound Minimum Bandwidth:
(0 - Max. Inbound Bandwidth Kbps)
Inbound Maximum Bandwidth:
(100 - 100000 Kbps)
Outbound Minimum Bandwidth:
(0 - Max. Outbound Bandwidth Kbps)
Outbound Maximum Bandwidth:
(100 - 100000 Kbps)
Type:
Group
Apply
Reset

Figure 74.

3. Enter the settings as explained in the following table:

Table 32. Add Bandwidth Profile screen settings

Setting	Description
Profile Name	A descriptive name of the bandwidth profile for identification and management purposes.
Direction	From the Direction drop-down list, select the traffic direction for the bandwidth profile: • **Inbound Traffic**. The bandwidth profile is applied only to inbound traffic. Specify the inbound minimum and maximum bandwidths. • **Outbound Traffic**. The bandwidth profile is applied only to outbound traffic. Specify the outbound minimum and maximum bandwidths. • **Both**. The bandwidth profile is applied to both outbound and inbound traffic. Specify both the outbound and inbound minimum and maximum bandwidths.

Table 32. Add Bandwidth Profile screen settings (continued)

Setting	Description
Inbound Minimum Bandwidth	The inbound minimum allocated bandwidth in Kbps. The default setting is 0 Kbps.
Inbound Maximum Bandwidth	The inbound maximum allowed bandwidth in Kbps. The default setting is 100 Kbps (you cannot configure less than 100 Kbps); the maximum allowable bandwidth is 100000 Kbps.
Outbound Minimum Bandwidth	The outbound minimum allocated bandwidth in Kbps. The default setting is 0 Kbps.
Outbound Maximum Bandwidth	The outbound maximum allowed bandwidth in Kbps. The default setting is 100 Kbps (you cannot configure less than 100 Kbps); the maximum allowable bandwidth is 100000 Kbps.
Type	From the Type drop-down list, select the type for the bandwidth profile: • **Group**. The profile applies to all users, that is, all users share the available bandwidth. • **Individual**. The profile applies to an individual user, that is, each user can use the available bandwidth.

4. Click **Apply** to save your settings. The new bandwidth profile is added to the List of Bandwidth Profiles table.

➢ **To edit a bandwidth profile:**

1. In the List of Bandwidth Profiles table, click the **Edit** table button to the right of the bandwidth profile that you want to edit. The Edit Bandwidth Profile screen displays.
2. Modify the settings that you wish to change (see the previous table).
3. Click **Apply** to save your changes. The modified bandwidth profile is displayed in the List of Bandwidth Profiles table.

➢ **To delete one or more bandwidth profiles:**

1. In the List of Bandwidth Profiles table, select the check box to the left of each bandwidth profile that you want to delete, or click the **Select All** table button to select all profiles.
2. Click the **Delete** table button to delete the selected profile or profiles.

Preconfigured Quality of Service Profiles

A Quality of Service (QoS) profile defines the relative priority of an IP packet when multiple connections are scheduled for simultaneous transmission on the wireless VPN firewall. A QoS profile becomes active only when it is associated with a nonblocking inbound or outbound firewall rule or service, and traffic matching the firewall rule or service is processed by the wireless VPN firewall. Priorities are defined by the Type of Service (ToS) in the Internet Protocol Suite standards, RFC 1349.

You can assign a QoS profile to a firewall rule or service on the following screens:

- Add LAN WAN Outbound Services screen (see *Figure 55* on page 118).
- Add DMZ WAN Outbound Services screen (see *Figure 58* on page 121).
- Services screen (see *Figure 71* on page 137)

These are the default QoS profiles that are preconfigured and that cannot be edited:

- **Normal-Service**. Used when no special priority is given to the traffic. IP packets are marked with a ToS value of 0.
- **Minimize-Cost**. Used when data needs to be transferred over a link that has a lower cost. IP packets are marked with a ToS value of 2.
- **Maximize-Reliability**. Used when data needs to travel to the destination over a reliable link and with little or no retransmission. IP packets are marked with a ToS value of 4.
- **Maximize-Throughput**. Used when the volume of data transferred during an interval is important even if the latency over the link is high. IP packets are marked with a ToS value of 8.
- **Minimize-Delay**. Used when the time required (latency) for the packet to reach the destination needs to be low. IP packets are marked with a ToS value of 16.

Configure Content Filtering

To restrict internal LAN users from access to certain sites on the Internet, you can use the content filtering and web component blocking features of the wireless VPN firewall. By default, these features are disabled; all requested traffic from any website is allowed. If you enable one or more of these features and users try to access a blocked site, they will see a “Blocked by NETGEAR” message.

Several types of blocking are available:

- **Web component blocking**. You can block the following web component types: proxy, Java, ActiveX, and cookies. Even sites that are listed in the Trusted Domains table are subject to web component blocking when the blocking of a particular web component is enabled.
  - **Proxy**. A proxy server (or simply, proxy) allows computers to route connections to other computers through the proxy, thus circumventing certain firewall rules. For example, if connections to a specific IP address are blocked by a firewall rule, the requests can be routed through a proxy that is not blocked by the rule, rendering the restriction ineffective. Enabling this feature blocks proxy servers.
  - **Java**. Blocks Java applets from being downloaded from pages that contain them. Java applets are small programs embedded in web pages that enable dynamic functionality of the page. A malicious applet can be used to compromise or infect computers. Enabling this setting blocks Java applets from being downloaded.

- **ActiveX**. Similar to Java applets, ActiveX controls are installed on a Windows computer running Internet Explorer. A malicious ActiveX control can be used to compromise or infect computers. Enabling this setting blocks ActiveX applets from being downloaded.
- **Cookies**. Cookies are used to store session information by websites that usually require login. However, several websites use cookies to store tracking information and browsing habits. Enabling this option blocks cookies from being created by a website.

Note: Many websites require that cookies be accepted in order for the site to be accessed correctly. Blocking cookies might interfere with useful functions provided by these websites.

- **Keyword blocking (domain name blocking)**. You can specify up to 32 words to block. If any of these words appear in the website name (URL) or in a newsgroup name, the website or newsgroup is blocked by the wireless VPN firewall.

  You can apply the keywords to one or more LAN groups. Requests from the PCs in the groups are blocked where keyword blocking has been enabled. Blocking does not occur for the PCs in the groups where keyword blocking has been disabled.

  You can bypass keyword blocking for trusted domains by adding the exact matching domain to the Trusted Domains table. Access to the domains or keywords on this list by PCs in the groups where keyword blocking has been enabled will be allowed to pass without any blocking.

  Keyword application examples:

  - If the keyword “xxx” is specified, the URL http://www.companycom/xxx.html is blocked, as is the newsgroup alt.pictures.xxx.
  - If the keyword “.com” is specified, only websites with other domain suffixes (such as .edu, .org, or .gov) can be viewed.
  - If you wish to block all Internet browsing access, enter **.** (period) as the keyword.

➢ **To enable and configure content filtering:**

1. Select **Security > Content Filtering**. The Block Sites screen displays. (The following figure shows some examples.)

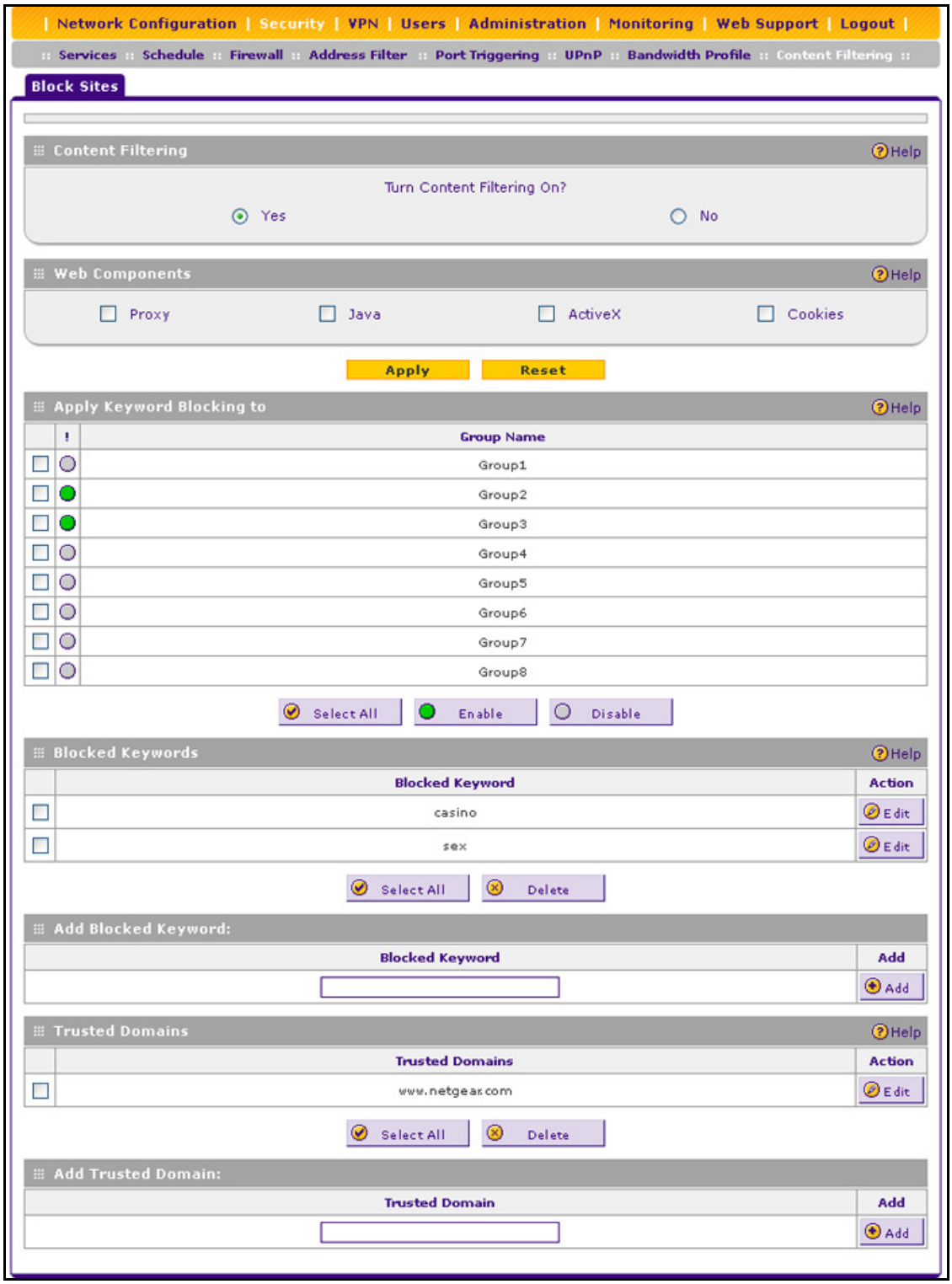


Figure 75.

2. In the Content Filtering section of the screen, select the **Yes** radio button.

3. In the Web Components section of the screen, select the components that you want to block:
   - **Proxy**. Blocks proxy servers.
   - **Java**. Blocks Java applets from being downloaded.
   - **ActiveX**. Blocks ActiveX applets from being downloaded.
   - **Cookies**. Blocks cookies from being created by a website.

   These components are explained in the introduction of this section on page 142.
4. Click **Apply** to enable content filtering and blocking of the selected web components. The screen controls are activated.

➢ **To apply keyword blocking to LAN groups:**

1. In the Apply Keyword Blocking to section of the screen, select the check boxes for the groups to which you want to apply keyword blocking, or click the **Select All** button to select all groups.
2. To activate keyword blocking for these groups, click the **Enable** button. To deactivate keyword blocking for the selected groups, click the **Disable** button.

Note: If you changed the LAN group names on the Edit Group Names screen (see *Change Group Names in the Network Database* on page 63), the default group names (Group1 through Group8) are displayed on the Content Filtering screen instead of the names that you specified on the Edit Group Names screen.

➢ **To build your list of blocked keywords or blocked domain names:**

1. In the Add Blocked Keyword section of the screen, in the Blocked Keyword field, enter a keyword or domain name.
2. After each entry, click the **Add** table button. The keyword or domain name is added to the Blocked Keywords table.

   To edit an entry, click the **Edit** table button in the Action column adjacent to the entry.

➢ **To build your list of trusted domains:**

1. In the Add Trusted Domain section of the screen, in the Trusted Domains field, enter a domain name.
2. After each entry, click the **Add** table button. The domain name is added to the Trusted Domains table.

   To edit an entry, click the **Edit** table button in the Action column adjacent to the entry.

Set a Schedule to Block or Allow Specific Traffic

Schedules define the time frames under which firewall rules can be applied. Three schedules, Schedule 1, Schedule 2, and Schedule 3, can be defined, and you can select any one of these when defining firewall rules.

➢ **To set a schedule:**

1. Select **Security > Services > Schedule 1**. The Schedule 1 screen displays:

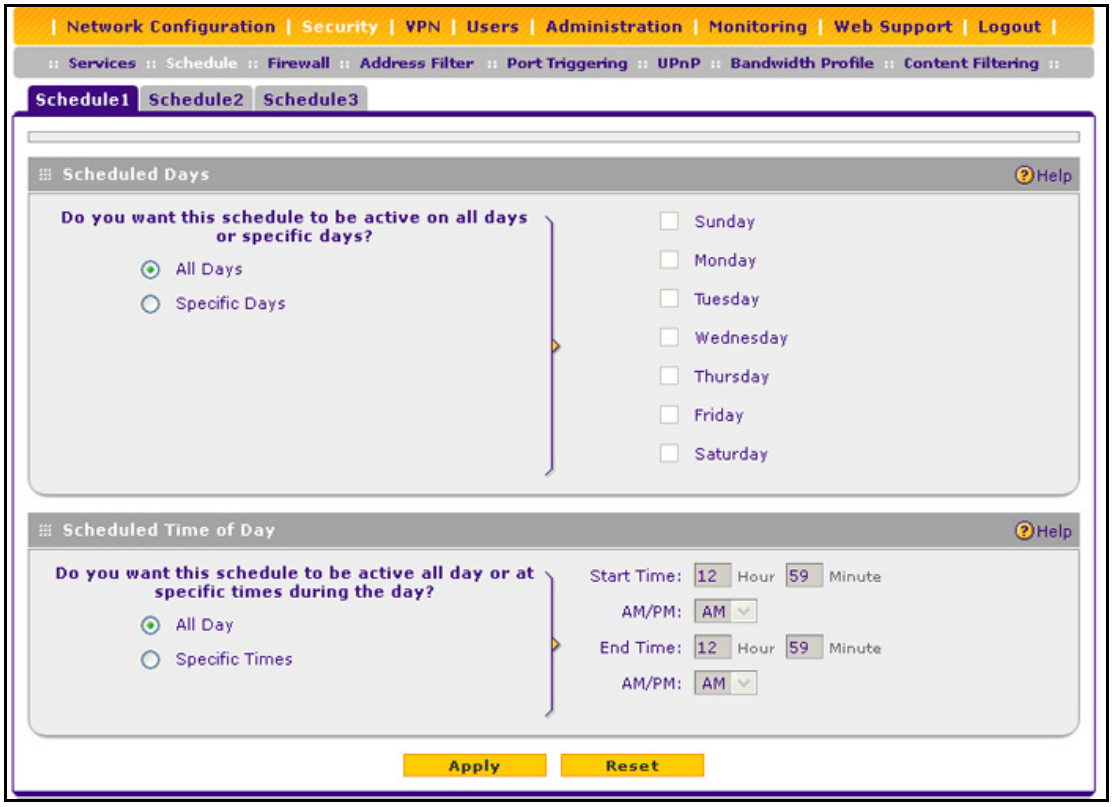

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering
Schedule1 Schedule2 Schedule3
Scheduled Days
Help
Do you want this schedule to be active on all days or specific days?
All Days
Specific Days
Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Scheduled Time of Day
Help
Do you want this schedule to be active all day or at specific times during the day?
All Day
Specific Times
Start Time: 12 Hour 59 Minute
AM/PM: AM
End Time: 12 Hour 59 Minute
AM/PM: AM
Apply
Reset

Figure 76.

2. In the Scheduled Days section, select one of the following radio buttons:
   - **All Days**. The schedule is in effect all days of the week.
   - **Specific Days**. The schedule is in effect only on specific days. To the right of the radio buttons, select the check box for each day that you want the schedule to be in effect.
3. In the Scheduled Time of Day section, select one of the following radio buttons:
   - **All Day**. The schedule is in effect all hours of the selected day or days.
   - **Specific Times**. The schedule is in effect only during specific hours of the selected day or days. To the right of the radio buttons, fill in the Start Time and End Time fields (Hour, Minute, AM/PM) during which the schedule is in effect.
4. Click **Apply** to save your settings to Schedule 1.

Repeat these steps to set to a schedule for Schedule 2 and Schedule 3.

Enable Source MAC Filtering

The Source MAC Filter screen enables you to permit or block traffic coming from certain known PCs or devices.

By default, the source MAC address filter is disabled. All the traffic received from PCs with any MAC address is allowed. When the source MAC address filter is enabled, depending on the selected policy, traffic is either permitted or blocked if it comes from any PCs or devices whose MAC addresses are listed in MAC Addresses table.

Note: For additional ways of restricting outbound traffic, see *Outbound Rules (Service Blocking)* on page 109.

➢ **To enable MAC filtering and add MAC addresses to be permitted or blocked:**

1. Select **Security > Address Filter**. The Address Filter submenu tabs display, with the Source MAC Filter screen in view. (The following figure shows one address in the MAC Addresses table as an example.)

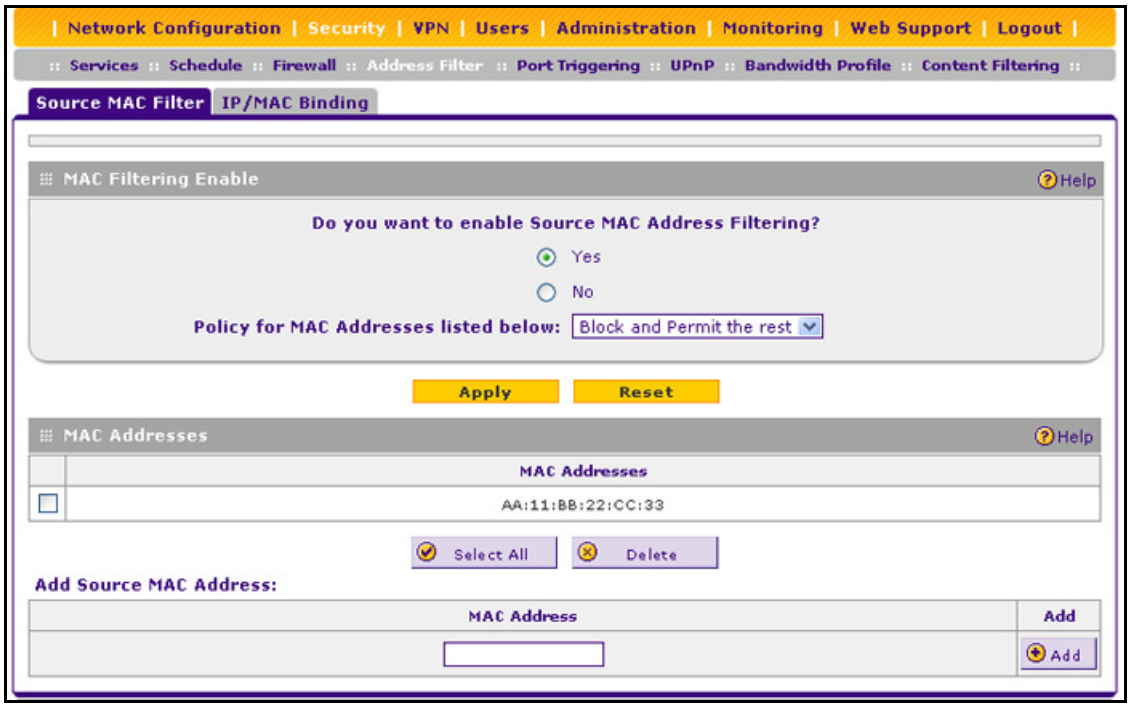


Figure 77.

2. In the MAC Filtering Enable section, select the **Yes** radio button.

3. In the same section, from the Policy for MAC Addresses listed below drop-down list, select one of the following options:
   - **Block and Permit the rest**. Traffic coming from all addresses in the MAC Addresses table is blocked. Traffic from all other MAC addresses is permitted.
   - **Permit and Block the rest**. Traffic coming from all addresses in the MAC Addresses table is permitted. Traffic from all other MAC addresses is blocked.
4. Click **Apply** to save your settings. The MAC Address field in the Add Source MAC Address section of the screen now becomes available.
5. Build your list of source MAC addresses to be permitted or blocked by entering the first MAC address in the MAC Address field. A MAC address needs to be entered in the format xx:xx:xx:xx:xx:xx, in which x is a numeric (0 to 9) or a letter between a and f (inclusive), for example: aa:11:bb:22:cc:33.

WARNING!

If you select Permit and Block the rest from the drop-down list but do not add the MAC address of the computer from which you are accessing the web management interface, you are locked out of the web management interface.

6. Click the **Add** table button. The MAC address is added to the MAC Addresses table.
7. Repeat the previous two steps to add more MAC addresses to the MAC Addresses table.

➢ **To remove one or more MAC addresses from the table:**

1. Select the check box to the left of each MAC address that you want to delete, or click the **Select All** table button to select all addresses.
2. Click the **Delete** table button.

Set Up IP/MAC Bindings

IP/MAC binding allows you to bind an IP address to a MAC address and the other way around. Some PCs or devices are configured with static addresses. To prevent users from changing their static IP addresses, the IP/MAC binding feature needs to be enabled on the wireless VPN firewall. If the wireless VPN firewall detects packets with an IP address that matches the IP address in the IP/MAC Bindings table but does not match the related MAC address in the IP/MAC Bindings table (or the other way around), the packets are dropped. If you have enabled the logging option for the IP/MAC binding feature, these packets are logged before they are dropped. The wireless VPN firewall displays the total number of dropped packets that violate either the IP-to-MAC binding or the MAC-to-IP binding.

Note: You can bind IP addresses to MAC addresses for DHCP assignment on the LAN Groups submenu. See *Manage the Network Database* on page 60.

As an example, assume that three computers on the LAN are set up as follows, and that their IP and MAC addresses are added to the IP/MAC Bindings table:

- Host 1. MAC address (00:01:02:03:04:05) and IP address (192.168.10.10)
- Host 2. MAC address (00:01:02:03:04:06) and IP address (192.168.10.11)
- Host 3. MAC address (00:01:02:03:04:07) and IP address (192.168.10.12)

There are three possible scenarios in relation to the addresses in the IP/MAC Bindings table:

- Host 1 has not changed its IP and MAC addresses. A packet coming from Host 1 has IP and MAC addresses that match those in the IP/MAC Bindings table.
- Host 2 has changed its MAC address to 00:01:02:03:04:09. The packet has an IP address that matches the IP address in the IP/MAC Bindings table but a MAC address that does not match the MAC address in the IP/MAC Bindings table.
- Host 3 has changed its IP address to 192.168.10.15. The packet has a MAC address that matches the MAC address in the IP/MAC Bindings table but an IP address that does not match the IP address in the IP/MAC Bindings table.

In this example, the wireless VPN firewall blocks the traffic coming from Host 2 and Host 3, but allows the traffic coming from Host 1 to any external network. The total count of dropped packets is displayed.

➢ **To set up IP/MAC bindings:**

1. Select **Security > Address Filter > IP/MAC Binding**. The IP/MAC Binding screen displays. (The following figure shows a binding in the IP/MAC Binding table as an example.)

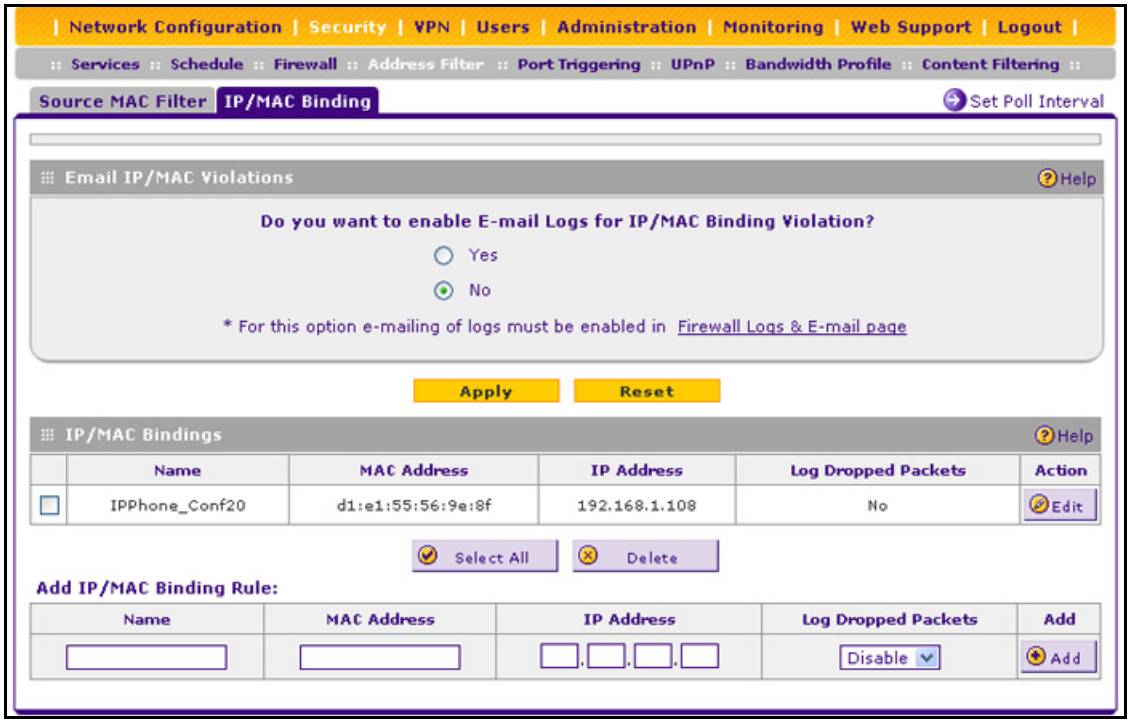


Figure 78.

2. Enter the settings as explained in the following table:

Table 33. IP/MAC Binding screen settings

Setting	Description
Email IP/MAC Violations	
Do you want to enable E-mail Logs for IP/MAC Binding Violation?	Select one of the following radio buttons: • **Yes**. IP/MAC binding violations are emailed. • **No**. IP/MAC binding violations are not emailed. **Note:** Click the **Firewall Logs & E-mail page** link to ensure that emailing of logs is enabled on the Firewall Logs & E-mail screen (see *Configure Logging, Alerts, and Event Notifications* on page 293).
IP/MAC Bindings	
Name	A descriptive name of the binding for identification and management purposes.
MAC Address	The MAC address of the PC or device that is bound to the IP address.
IP Address	The IP address of the PC or device that is bound to the MAC address.
Log Dropped Packets	To log the dropped packets, select **Enable** from the drop-down list. The default setting is Disable.

3. Click the **Add** table button. The new IP/MAC rule is added to the IP/MAC Bindings table.
4. Click **Apply** to save your changes.

➢ **To edit an IP/MAC binding:**

1. In the IP/MAC Bindings table, click the **Edit** table button to the right of the IP/MAC binding that you want to edit. The Edit IP/MAC Binding screen displays.
2. Modify the settings that you wish to change (see the previous table).
3. Click **Apply** to save your changes. The modified IP/MAC binding displays in the IP/MAC Bindings table.

➢ **To remove one or more IP/MAC bindings from the table:**

1. Select the check box to the left of each IP/MAC binding that you want to delete, or click the **Select All** table button to select all bindings.
2. Click the **Delete** table button.

Configure Port Triggering

Port triggering allows some applications running on a LAN network to be available to external applications that would otherwise be partially blocked by the firewall. Using the port-triggering feature requires that you know the port numbers used by the application.

Once configured, port triggering operates as follows:

1. A PC makes an outgoing connection using a port number that is defined in the Port Triggering Rules table.
2. The wireless VPN firewall records this connection, opens the additional incoming port or ports that are associated with the rule in the port triggering table, and associates them with the PC.
3. The remote system receives the PC's request and responds using the incoming port or ports that are associated with the rule in the port triggering table on the wireless VPN firewall.
4. The wireless VPN firewall matches the response to the previous request and forwards the response to the PC.

Without port triggering, the response from the external application would be treated as a new connection request rather than a response to a request from the LAN network. As such, it would be handled in accordance with the inbound port-forwarding rules, and most likely would be blocked.

Note these restrictions on port triggering:

- Only one PC can use a port-triggering application at any time.
- After a PC has finished using a port-triggering application, there is a short time-out period before the application can be used by another PC. This time-out period is required so the wireless VPN firewall can determine that the application has terminated.

Note: For additional ways of allowing inbound traffic, see *Inbound Rules (Port Forwarding)* on page 112.

➢ **To add a port-triggering rule:**

1. Select **Security > Port Triggering**. The Port Triggering screen displays. (The following figure shows a rule in the Port Triggering Rule table as an example.)

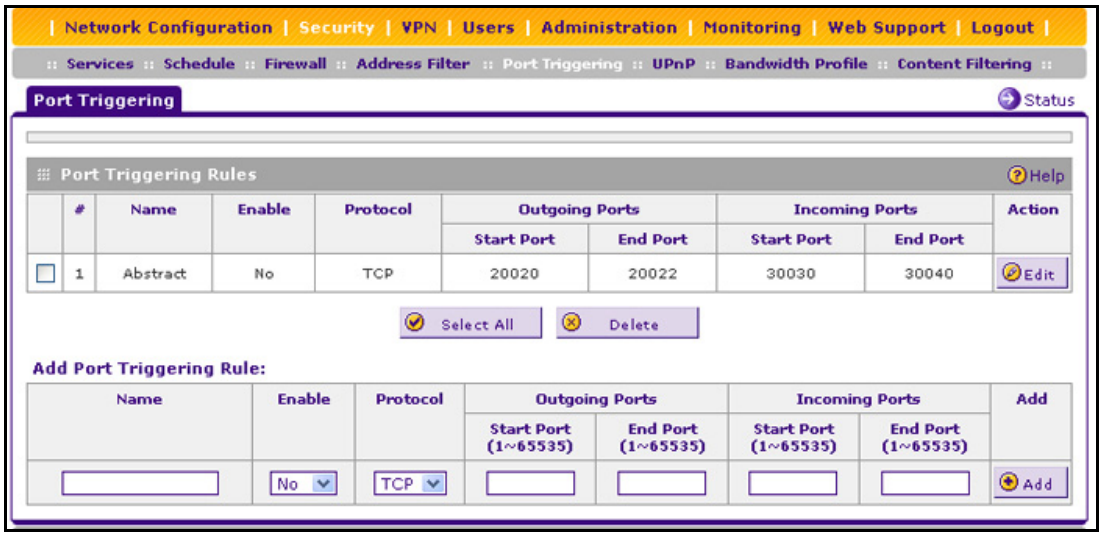

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering
Port Triggering
Status
Port Triggering Rules
Help
Name Enable Protocol Outgoing Ports Incoming Ports Action
Start Port End Port Start Port End Port
1 Abstract No TCP 20020 20022 30030 30040 Edit
Select All
Delete
Add Port Triggering Rule:
Name Enable Protocol Outgoing Ports Incoming Ports Add
Start Port (1~65535) End Port (1~65535) Start Port (1~65535) End Port (1~65535)
No
TCP
Add

Figure 79.

2. In the Add Port Triggering Rule section, enter the settings as explained in the following table:

Table 34. Port Triggering screen settings

Setting	Description	
Name	A descriptive name of the rule for identification and management purposes.	
Enable	From the drop-down list, select **Yes** to enable the rule. (You can define a rule but not enable it.) The default setting is No.	
Protocol	From the drop-down list, select the protocol to which the rule applies: • **TCP**. The rule applies to an application that uses the Transmission Control Protocol (TCP). • **UDP**. The rule applies to an application that uses the User Datagram Protocol (UDP).	
Outgoing (Trigger) Port Range	Start Port	The start port (1–65535) of the range for triggering.
	End Port	The end port (1–65535) of the range for triggering.
Incoming (Response) Port Range	Start Port	The start port (1–65535) of the range for responding.
	End Port	The end port (1–65535) of the range for responding.

3. Click the **Add** table button. The new port-triggering rule is added to the Port Triggering Rules table.

➢ **To edit a port-triggering rule:**

1. In the Port Triggering Rules table, click the **Edit** table button to the right of the port-triggering rule that you want to edit. The Edit Port Triggering Rule screen displays.
2. Modify the settings that you wish to change (see the previous table).
3. Click **Apply** to save your changes. The modified port-triggering rule is displayed in the Port Triggering Rules table.

➢ **To remove one or more port-triggering rules from the table:**

1. Select the check box to the left of each port-triggering rule that you want to delete, or click the **Select All** table button to select all rules.
2. Click the **Delete** table button.

➢ **To display the status of the port-triggering rules:**

Click the **Status** option arrow in the upper right of the Port Triggering screen. A pop-up screen displays, showing the status of the port-triggering rules.

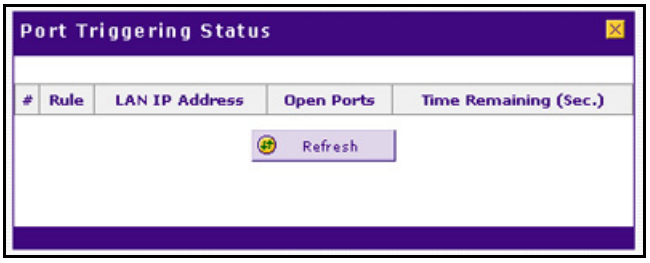


Figure 80.

Configure Universal Plug and Play

The Universal Plug and Play (UPnP) feature enables the wireless VPN firewall to automatically discover and configure devices when it searches the LAN and WAN.

➢ **To configure UPnP:**

1. Select **Security > UPnP**. The UPnP screen displays:

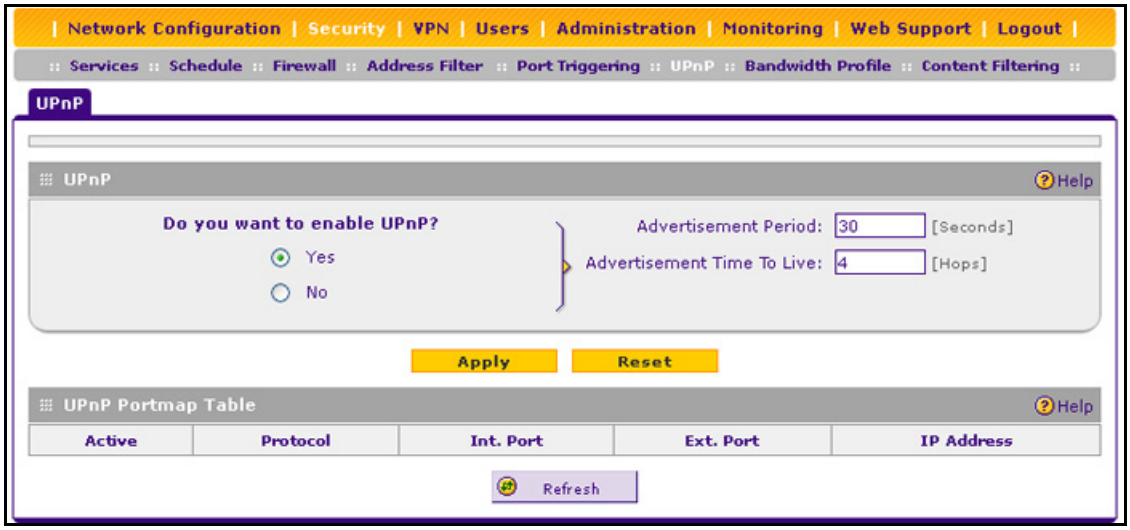


Figure 81.

The UPnP Portmap Table in the lower part of the screen shows the IP addresses and other settings of UPnP devices that have accessed the wireless VPN firewall and that have been automatically detected by the wireless VPN firewall:

- **Active**. A Yes or No indicates if the UPnP device port that established a connection is currently active.
- **Protocol**. Indicates the network protocol such as HTTP or FTP that is used by the device to connect to the VPN firewall.
- **Int. Port**. Indicates if any internal ports are opened by the UPnP device.
- **Ext. Port**. Indicates if any external ports are opened by the UPnP device.
- **IP Address**. Lists the IP address of the UPnP device accessing the VPN firewall.

2. To enable the UPnP feature, select the **Yes** radio button. (The feature is disabled by default.) To disable the feature, select **No**.
3. Fill in the following fields:
   - **Advertisement Period**. Enter the period in seconds that specifies how often the wireless VPN firewall should broadcast its UPnP information to all devices within its range. The default setting is 30 seconds.
   - **Advertisement Time to Live**. Enter a number that specifies how many steps (hops) each UPnP packet is allowed to propagate before being discarded. Small values will limit the UPnP broadcast range. The default setting is 4 hops.
4. Click **Apply** to save your settings.

To refresh the contents of the UPnP Portmap Table, click **Refresh**.

Virtual Private Networking Using IPv4 IPSec and L2TP Connections

6

This chapter describes how to use the IP security (IPSec) virtual private networking (VPN) features of the wireless VPN firewall to provide secure, encrypted communications between your local network and a remote network or computer. This chapter contains the following sections:

- *Use the IPSec VPN Wizard for Client and Gateway Configurations*
- *Test the Connection and View Connection and Status Information*
- *Manage IPSec VPN Policies*
- *Configure Extended Authentication (XAUTH)*
- *Assign IP Addresses to Remote Users (Mode Config)*
- *Configure Keep-Alives and Dead Peer Detection*
- *Configure NetBIOS Bridging with IPSec VPN*
- *Configure the L2TP Server*

Note: In this release, the wireless VPN firewall supports IPSec VPN connections for IPv4 traffic only. By themselves IPv6 addresses provide a much higher level of security than IPv4 addresses, and future releases will support IPSec VPN connections for IPv6 traffic.

Use the IPSec VPN Wizard for Client and Gateway Configurations

You can use the IPSec VPN Wizard to configure multiple gateway or client VPN tunnel policies.

The following section provides wizard and NETGEAR ProSafe VPN Client software configuration procedures for the following scenarios:

- Using the wizard to configure a VPN tunnel between two VPN gateways
- Using the wizard to configure a VPN tunnel between a VPN gateway and a VPN client

Configuring a VPN tunnel connection requires that you specify all settings on both sides of the VPN tunnel to match or mirror each other precisely, which can be a daunting task. The VPN Wizard efficiently guides you through the setup procedure with a series of questions that determine the IPSec keys and VPN policies it sets up. The VPN Wizard also configures the settings for the network connection: security association (SA), traffic selectors, authentication algorithm, and encryption. The settings that are used by the VPN Wizard are based on the recommendations of the VPN Consortium (VPNC), an organization that promotes multivendor VPN interoperability.

Create a Gateway-to-Gateway VPN Tunnel with the Wizard

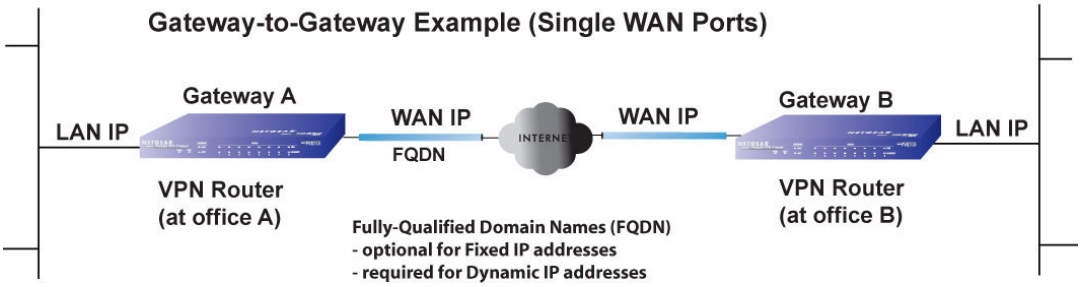


Figure 82.

➢ **To set up a gateway-to-gateway VPN tunnel using the VPN Wizard:**

1. Select **VPN > IPSec VPN > VPN Wizard**. The VPN Wizard screen displays. (The following screen contains some examples that do not relate to other examples in this manual.)

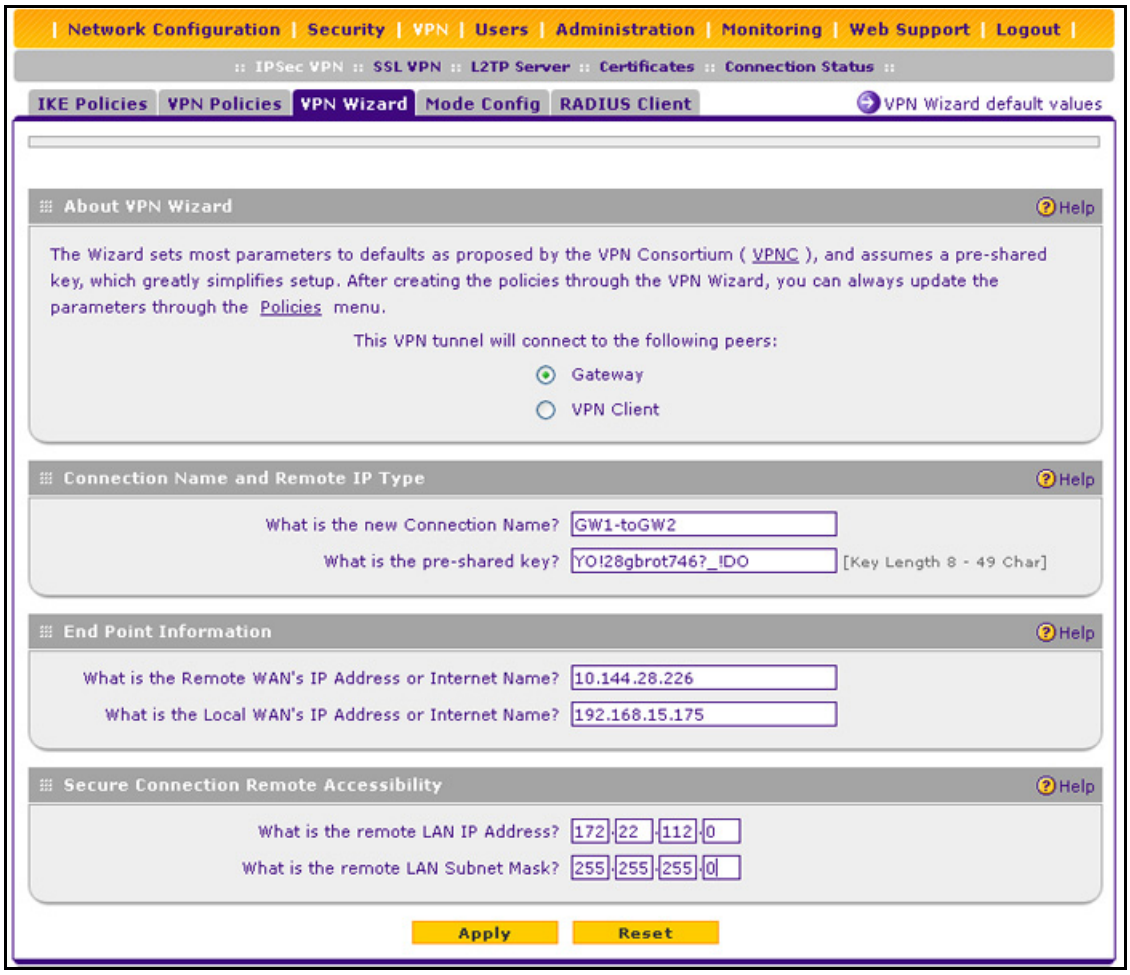

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
IPSec VPN :: SSL VPN :: L2TP Server :: Certificates :: Connection Status
IKE Policies
VPN Policies
VPN Wizard
Mode Config
RADIUS Client
VPN Wizard default values
About VPN Wizard
Help
The Wizard sets most parameters to defaults as proposed by the VPN Consortium (VPNC), and assumes a pre-shared key, which greatly simplifies setup. After creating the policies through the VPN Wizard, you can always update the parameters through the Policies menu.
This VPN tunnel will connect to the following peers:
Gateway
VPN Client
Connection Name and Remote IP Type
Help
What is the new Connection Name?
GW1-toGW2
What is the pre-shared key?
YO!28gbrot746?_!DO
[Key Length 8 - 49 Char]
End Point Information
Help
What is the Remote WAN's IP Address or Internet Name?
10.144.28.226
What is the Local WAN's IP Address or Internet Name?
192.168.15.175
Secure Connection Remote Accessibility
Help
What is the remote LAN IP Address?
172 . 22 . 112 . 0
What is the remote LAN Subnet Mask?
255 . 255 . 255 . 0
Apply
Reset

Figure 83.

To view the wizard default settings, click the **VPN Wizard Default Values** option arrow in the upper right of the screen. A pop-up screen displays (see the following figure), showing the wizard default values.

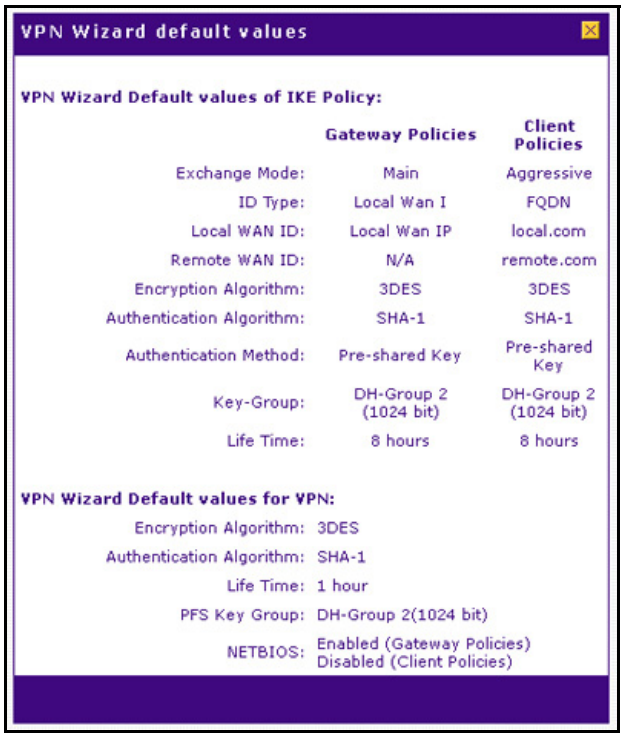

VPN Wizard default values
VPN Wizard Default values of IKE Policy:
Gateway Policies
Client Policies
Exchange Mode: Main Aggressive
ID Type: Local Wan I FQDN
Local WAN ID: Local Wan IP local.com
Remote WAN ID: N/A remote.com
Encryption Algorithm: 3DES 3DES
Authentication Algorithm: SHA-1 SHA-1
Authentication Method: Pre-shared Key Pre-shared Key
Key-Group: DH-Group 2 (1024 bit) DH-Group 2 (1024 bit)
Life Time: 8 hours 8 hours
VPN Wizard Default values for VPN:
Encryption Algorithm: 3DES
Authentication Algorithm: SHA-1
Life Time: 1 hour
PFS Key Group: DH-Group 2(1024 bit)
NETBIOS: Enabled (Gateway Policies) Disabled (Client Policies)

Figure 84.

2. Complete the settings as explained in the following table:

Table 35. IPSec VPN Wizard settings for a gateway-to-gateway tunnel

Setting	Description
About VPN Wizard	
This VPN tunnel will connect to the following peers	Select the **Gateway** radio button. The local WAN port's IP address or Internet name displays in the End Point Information section of the screen.
Connection Name and Remote IP Type	
What is the new Connection Name?	Enter a descriptive name for the connection. This name is used to help you to manage the VPN settings; the name is not supplied to the remote VPN endpoint.
What is the pre-shared key?	Enter a pre-shared key. The key needs to be entered both here and on the remote VPN gateway. This key needs to have a minimum length of 8 characters and should not exceed 49 characters.
End Point Information[a]	
What is the Remote WAN's IP Address or Internet Name?	Enter the IP address or Internet name (FQDN) of the WAN interface on the remote VPN tunnel endpoint.
What is the Local WAN's IP Address or Internet Name?	When you select the Gateway radio button in the About VPN Wizard section of the screen, the IP address of the wireless VPN firewall's active WAN interface is automatically entered.

Table 35. IPSec VPN Wizard settings for a gateway-to-gateway tunnel (continued)

Setting	Description
Secure Connection Remote Accessibility	
What is the remote LAN IP Address?	Enter the LAN IP address of the remote gateway. **Note:** The remote LAN IP address needs to be in a different subnet than the local LAN IP address. For example, if the local subnet is 192.168.1.x, then the remote subnet could be 192.168.10.x. but could not be 192.168.1.x. If this information is incorrect, the tunnel will fail to connect.
What is the remote LAN Subnet Mask?	Enter the LAN subnet mask of the remote gateway.

a. Both local and remote endpoints should be defined as either FQDNs or IP addresses. A combination of an IP address and an FQDN is not supported.

Tip: To ensure that tunnels stay active, after completing the wizard, manually edit the VPN policy to enable keep-alives, which periodically sends ping packets to the host on the peer side of the network to keep the tunnel alive. For more information, see *Configure Keep-Alives* on page 215.

Tip: For DHCP WAN configurations, first set up the tunnel with IP addresses. After you have validated the connection, you can use the wizard to create new policies using the FQDN for the WAN addresses.

3. Click **Apply** to save your settings. The IPSec VPN policy is now added to the List of VPN Policies table on the VPN Policies screen. By default, the VPN policy is enabled.

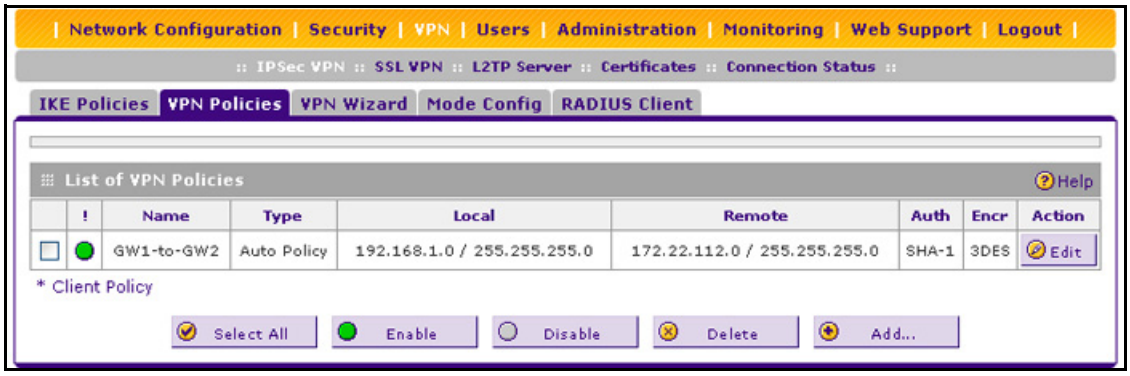

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
IPSec VPN :: SSL VPN :: L2TP Server :: Certificates :: Connection Status
IKE Policies
VPN Policies
VPN Wizard
Mode Config
RADIUS Client
List of VPN Policies
Help
! Name Type Local Remote Auth Encr Action
GW1-to-GW2 Auto Policy 192.168.1.0 / 255.255.255.0 172.22.112.0 / 255.255.255.0 SHA-1 3DES Edit
* Client Policy
Select All
Enable
Disable
Delete
Add...

Figure 85.

4. Configure a VPN policy on the remote gateway that allows connection to the wireless VPN firewall.
5. Activate the IPSec VPN connection:
   a. Select **VPN > Connection Status > IPSec VPN Connection Status**. The IPSec VPN Connection Status screen displays:

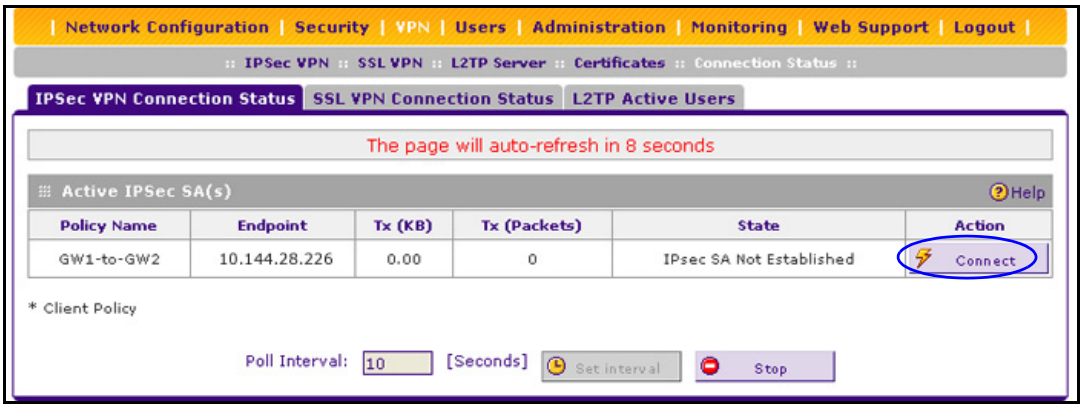


Figure 86.

b. Locate the policy in the table, and click the **Connect** table button. The IPSec VPN connection becomes active.

Note: When using FQDNs, if the Dynamic DNS service is slow to update its servers when your DHCP WAN address changes, the VPN tunnel will fail because the FQDNs do not resolve to your new address. If you have the option to configure the update interval, set it to an appropriately short time.

Create a Client-to-Gateway VPN Tunnel

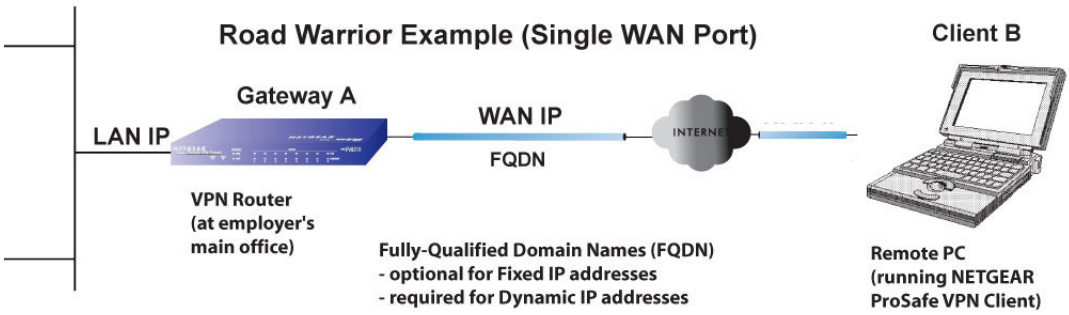


Figure 87.

To configure a VPN client tunnel, follow the steps in the following sections:

- *Use the VPN Wizard to Configure the Gateway for a Client Tunnel* on page 161.
- *Use the NETGEAR VPN Client Wizard to Create a Secure Connection* on page 163 *or* *Manually Create a Secure Connection Using the NETGEAR VPN Client* on page 168.

Use the VPN Wizard to Configure the Gateway for a Client Tunnel

➢ **To set up a client-to-gateway VPN tunnel using the VPN Wizard:**

1. Select **VPN > IPSec VPN > VPN Wizard**. The VPN Wizard screen displays. (The following figure contains an example.)

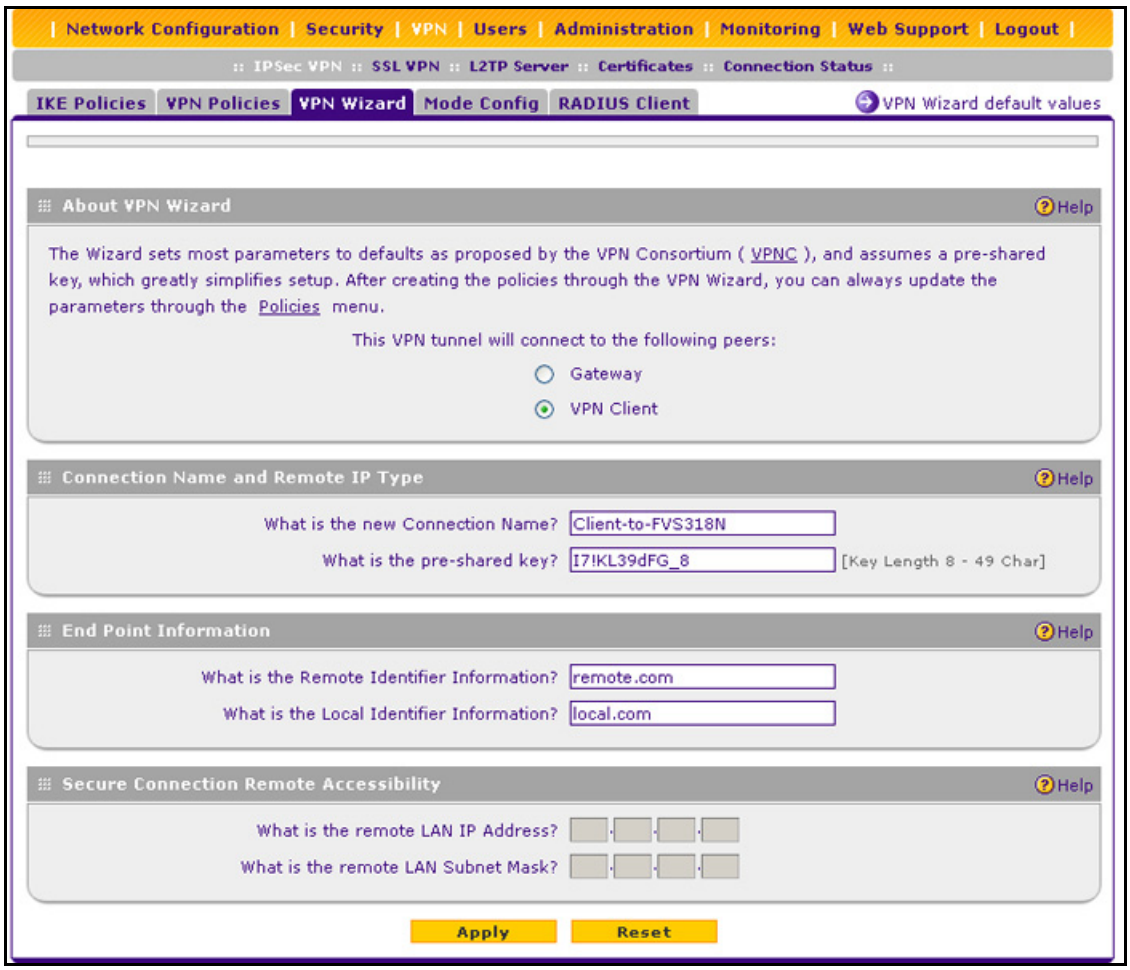

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
IPSec VPN :: SSL VPN :: L2TP Server :: Certificates :: Connection Status
IKE Policies | VPN Policies | VPN Wizard | Mode Config | RADIUS Client
VPN Wizard default values
About VPN Wizard
Help
The Wizard sets most parameters to defaults as proposed by the VPN Consortium (VPNC), and assumes a pre-shared key, which greatly simplifies setup. After creating the policies through the VPN Wizard, you can always update the parameters through the Policies menu.
This VPN tunnel will connect to the following peers:
Gateway
VPN Client
Connection Name and Remote IP Type
Help
What is the new Connection Name?
Client-to-FVS318N
What is the pre-shared key?
I7!KL39dFG_8
[Key Length 8 - 49 Char]
End Point Information
Help
What is the Remote Identifier Information?
remote.com
What is the Local Identifier Information?
local.com
Secure Connection Remote Accessibility
Help
What is the remote LAN IP Address?
What is the remote LAN Subnet Mask?
Apply
Reset

Figure 88.

To display the wizard default settings, click the **VPN Wizard default values** option arrow in the upper right of the screen. A pop-up screen displays (see *Figure 84* on page 158), showing the wizard default values. After you have completed the wizard, you can modify these settings for the tunnel policy that you have set up.

2. Complete the settings as explained in the following table:

Table 36. IPSec VPN Wizard settings for a client-to-gateway tunnel

Setting	Description
About VPN Wizard	
This VPN tunnel will connect to the following peers	Select the **VPN Client** radio button. The default remote FQDN (remote.com) and the default local FQDN (local.com) display in the End Point Information section of the screen.
Connection Name and Remote IP Type	
What is the new Connection Name?	Enter a descriptive name for the connection. This name is used to help you to manage the VPN settings; the name is not supplied to the remote VPN endpoint.
What is the pre-shared key?	Enter a pre-shared key. The key needs to be entered both here and on the remote VPN gateway, or the remote VPN client. This key needs to have a minimum length of 8 characters and cannot exceed 49 characters.
End Point Information[a]	
What is the Remote Identifier Information?	When you select the Client radio button in the About VPN Wizard section of the screen, the default remote FQDN (remote.com) is automatically entered. Use the default remote FQDN, or enter another FQDN. **Note:** The remote ID on the wireless VPN firewall is the local ID on the VPN client. It might be less confusing to configure an FQDN such as client.com as the remote ID on the wireless VPN firewall and then enter client.com as the local ID on the VPN client.
What is the Local Identifier Information?	When you select the Client radio button in the About VPN Wizard section of the screen, the default local FQDN (local.com) is automatically entered. Use the default local FQDN, or enter another FQDN. **Note:** The local ID on the wireless VPN firewall is the remote ID on the VPN client. It might be less confusing to configure an FQDN such as router.com as the local ID on the wireless VPN firewall and then enter router.com as the remote ID on the VPN client.
Secure Connection Remote Accessibility	
What is the remote LAN IP Address?	These fields are masked out for VPN client connections.
What is the remote LAN Subnet Mask?	

a. Both local and remote endpoints should be defined as either FQDNs or IP addresses. A combination of an IP address and an FQDN is not supported.

3. Click **Apply** to save your settings. The IPSec VPN policy is now added to the List of VPN Policies table on the VPN Policies screen. By default, the VPN policy is enabled.

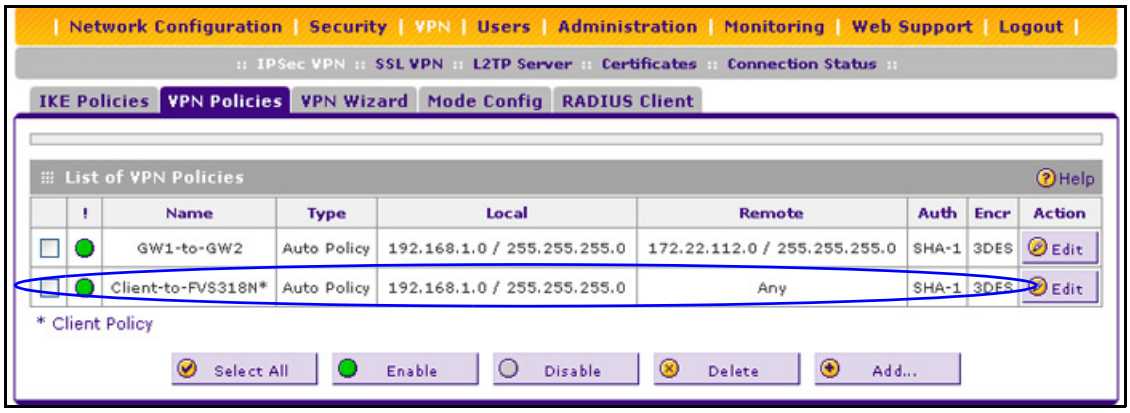

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
IPSec VPN :: SSL VPN :: L2TP Server :: Certificates :: Connection Status
IKE Policies
VPN Policies
VPN Wizard
Mode Config
RADIUS Client
List of VPN Policies
Help
! Name Type Local Remote Auth Encr Action
GW1-to-GW2 Auto Policy 192.168.1.0 / 255.255.255.0 172.22.112.0 / 255.255.255.0 SHA-1 3DES Edit
Client-to-FVS318N* Auto Policy 192.168.1.0 / 255.255.255.0 Any SHA-1 3DES Edit
* Client Policy
Select All
Enable
Disable
Delete
Add...

Figure 89.

Note: When you are using FQDNs, if the Dynamic DNS service is slow to update its servers when your DHCP WAN address changes, the VPN tunnel will fail because the FQDNs do not resolve to your new address. If you have the option to configure the update interval, set it to an appropriately short time.

4. Optional step: Collect the information that you need to configure the VPN client. You can print the following table to help you keep track of this information.

Table 37. Information required to configure the VPN client

Component	Example	Information to be collected
Pre-shared key	I7!KL39dFG_8	
Remote identifier information	remote.com	
Local identifier information	local.com	
Router's LAN network IP address	192.168.1.0	
Router's LAN network mask	255.255.255.0	
Router's WAN IP address	192.168.15.175	

Use the NETGEAR VPN Client Wizard to Create a Secure Connection

The VPN client lets you set up the VPN connection manually (see *Manually Create a Secure Connection Using the NETGEAR VPN Client* on page 168) or with the integrated Configuration Wizard, which is the easier and preferred method. The Configuration Wizard configures the default settings and provides basic interoperability so that the VPN client can easily communicate with the wireless VPN firewall (or third-party VPN devices). The Configuration Wizard does not let you enter the local and remote IDs, so you need to manually enter this information.

Note: Perform these tasks from a PC that has the NETGEAR ProSafe VPN Client installed.

➢ **To use the Configuration Wizard to set up a VPN connection between the VPN client and the wireless VPN firewall:**

1. Right-click the VPN client icon in your Windows system tray, and select **Configuration Panel**. The Configuration Panel screen displays.

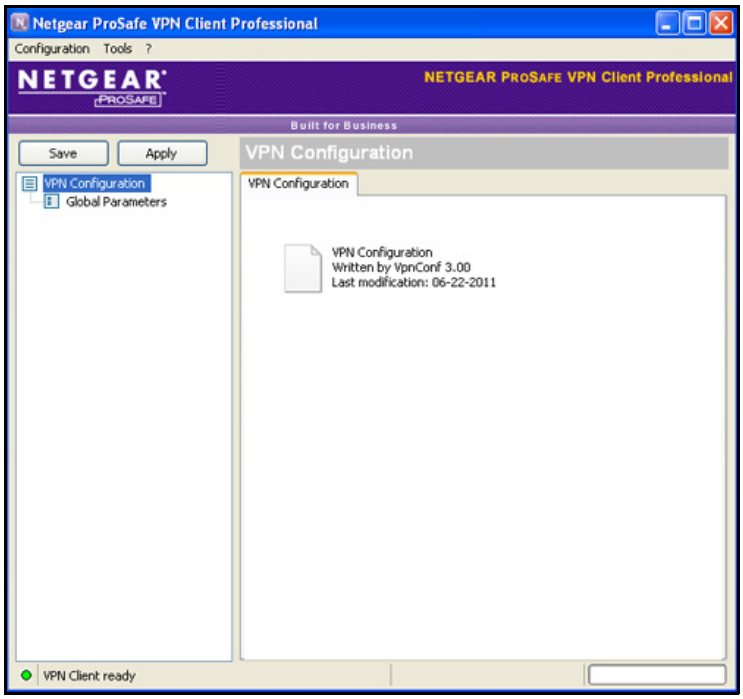


Figure 90.

1. From the main menu on the Configuration Panel screen, select **Configuration > Wizard**. The Choice of the remote equipment wizard screen (screen 1 of 3) displays.

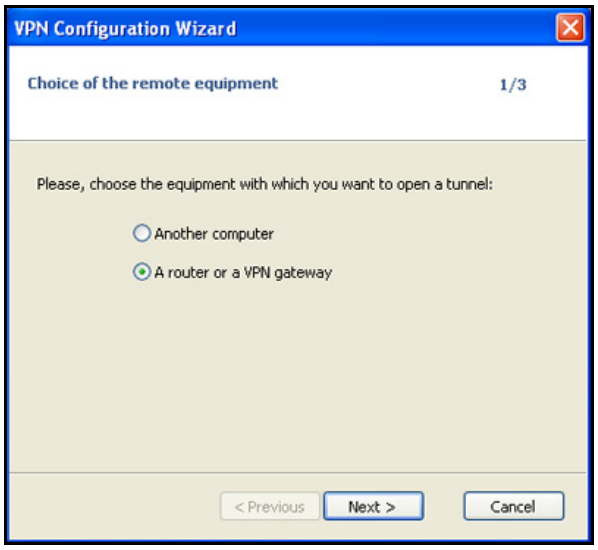

VPN Configuration Wizard
Choice of the remote equipment
1/3
Please, choose the equipment with which you want to open a tunnel:
Another computer
A router or a VPN gateway
< Previous
Next >
Cancel

Figure 91.

2. Select the **A router or a VPN gateway** radio button, and click **Next**. The VPN tunnel parameters wizard screen (screen 2 of 3) displays.

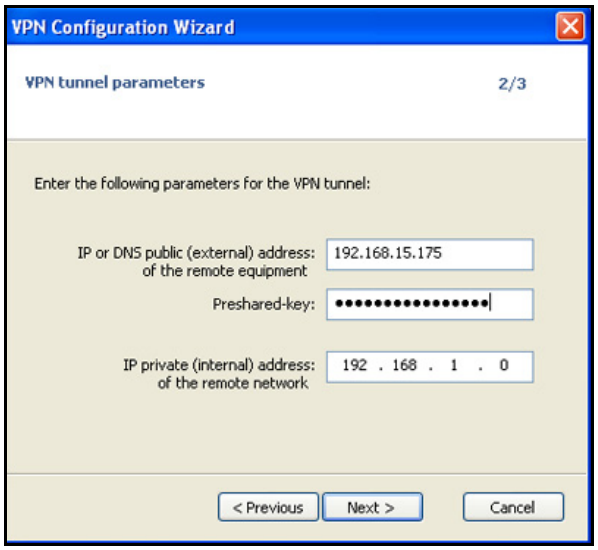

VPN Configuration Wizard
VPN tunnel parameters
2/3
Enter the following parameters for the VPN tunnel:
IP or DNS public (external) address: of the remote equipment
192.168.15.175
Preshared-key:
IP private (internal) address: of the remote network
192 . 168 . 1 . 0
< Previous
Next >
Cancel

Figure 92.

3. Specify the following VPN tunnel parameters:
   - **IP or DNS public (external) address of the remote equipment**. Enter the remote IP address or DNS name of the wireless VPN firewall. For example, enter **192.168.15.175**.
   - **Preshared key**. Enter the pre-shared key that you already specified on the wireless VPN firewall. For example, enter **I7!KL39dFG_8**.
   - **IP private (internal) address of the remote network**. Enter the remote private IP address of the wireless VPN firewall. For example, enter **192.168.1.0**. This IP address enables communication with the entire 192.168.1.x subnet.

4. Click **Next**. The Configuration Summary wizard screen (screen 3 of 3) displays.

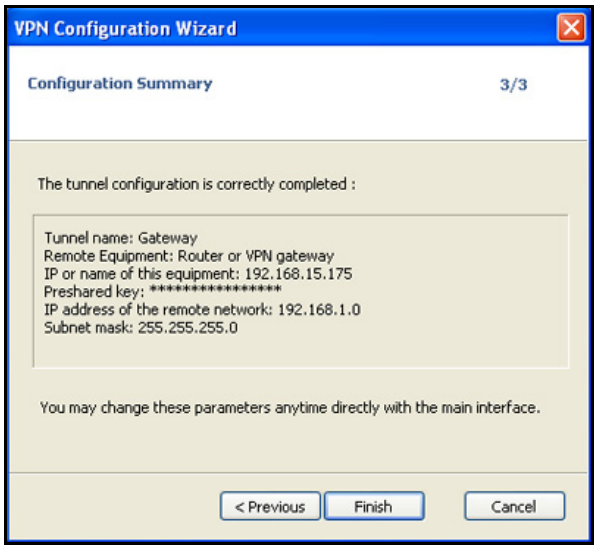

VPN Configuration Wizard
Configuration Summary
3/3
The tunnel configuration is correctly completed :
Tunnel name: Gateway
Remote Equipment: Router or VPN gateway
IP or name of this equipment: 192.168.15.175
Preshared key: **********
IP address of the remote network: 192.168.1.0
Subnet mask: 255.255.255.0
You may change these parameters anytime directly with the main interface.
< Previous
Finish
Cancel

Figure 93.

5. This screen is a summary screen of the new VPN configuration. Click **Finish**.
6. Specify the local and remote IDs:
   a. In the tree list pane of the Configuration Panel screen, click **Gateway** (the default name given to the authentication phase). The Authentication pane displays in the Configuration Panel screen, with the Authentication tab selected by default.
   b. Click the **Advanced** tab in the Authentication pane. The Advanced pane displays.

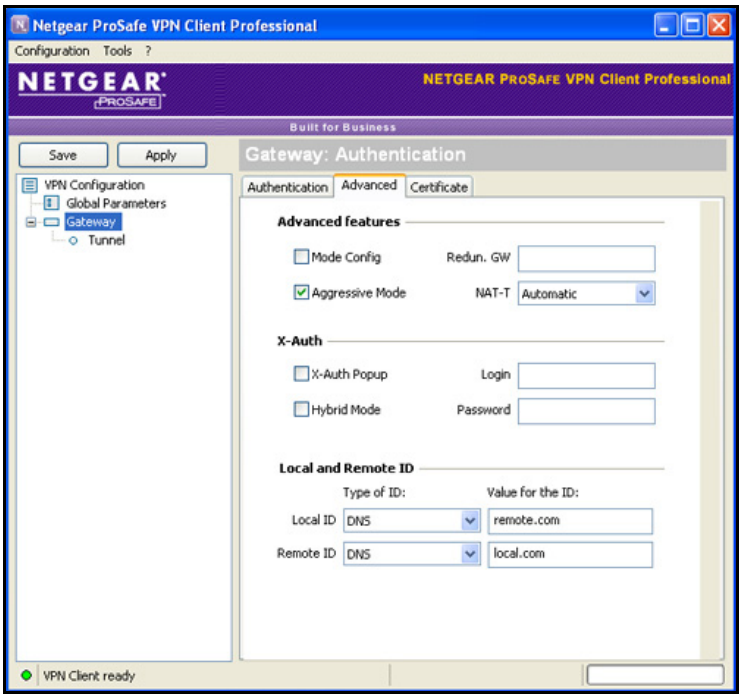


Figure 94.

c. Specify the settings that are explained in the following table.

Table 38. VPN client advanced authentication settings

Setting	Description
Advanced features	
Aggressive Mode	Select this check box to enable aggressive mode as the mode of negotiation with the wireless VPN firewall.
NAT-T	Select **Automatic** from the drop-down list to enable the VPN client and wireless VPN firewall to negotiate NAT-T.
Local and Remote ID	
Local ID	As the type of ID, select **DNS** from the Local ID drop-down list because you specified FQDN in the wireless VPN firewall configuration. As the value of the ID, enter **remote.com** as the local ID for the VPN client. **Note:** The remote ID on the wireless VPN firewall is the local ID on the VPN client. It might be less confusing to configure an FQDN such as client.com as the remote ID on the wireless VPN firewall and then enter client.com as the local ID on the VPN client.
Remote ID	As the type of ID, select **DNS** from the Remote ID drop-down list because you specified an FQDN in the wireless VPN firewall configuration. As the value of the ID, enter **local.com** as the remote ID for the wireless VPN firewall. **Note:** The local ID on the wireless VPN firewall is the remote ID on the VPN client. It might be less confusing to configure an FQDN such as router.com as the local ID on the wireless VPN firewall and then enter router.com as the remote ID on the VPN client.

7. Configure the global parameters:

   a. Click **Global Parameters** in the left column of the Configuration Panel screen. The Global Parameters pane displays in the Configuration Panel screen.

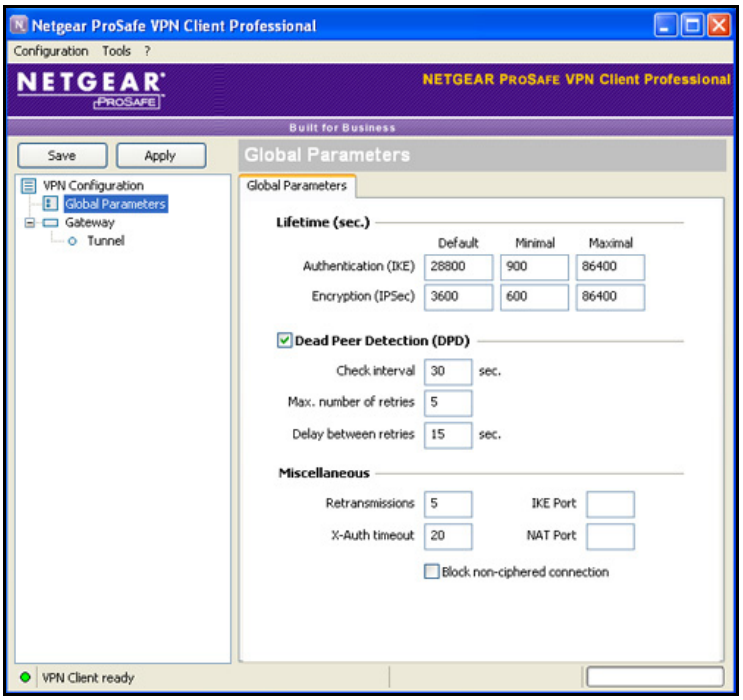


Figure 95.

b. Specify the default lifetimes in seconds:

- **Authentication (IKE)**, **Default**. The default lifetime value is 3600 seconds. Change this setting to **28800** seconds to match the configuration of the wireless VPN firewall.
- **Encryption (IPSec)**, **Default**. The default lifetime value is 1200 seconds. Change this setting to **3600** seconds to match the configuration of the wireless VPN firewall.

8. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.

The VPN client configuration is now complete.

Instead of using the wizard on the VPN client, you can also manually configure the VPN client, which is explained in the following section.

Manually Create a Secure Connection Using the NETGEAR VPN Client

Note: Perform these tasks from a PC that has the NETGEAR ProSafe VPN Client installed.

To manually configure a VPN connection between the VPN client and the wireless VPN firewall, create authentication settings (phase 1 settings), create an associated IPSec configuration (phase 2 settings), and then specify the global parameters.

Configure the Authentication Settings (Phase 1 Settings)

➢ **To create new authentication settings:**

1. Right-click the VPN client icon in your Windows system tray, and select **Configuration Panel**. The Configuration Panel screen displays.

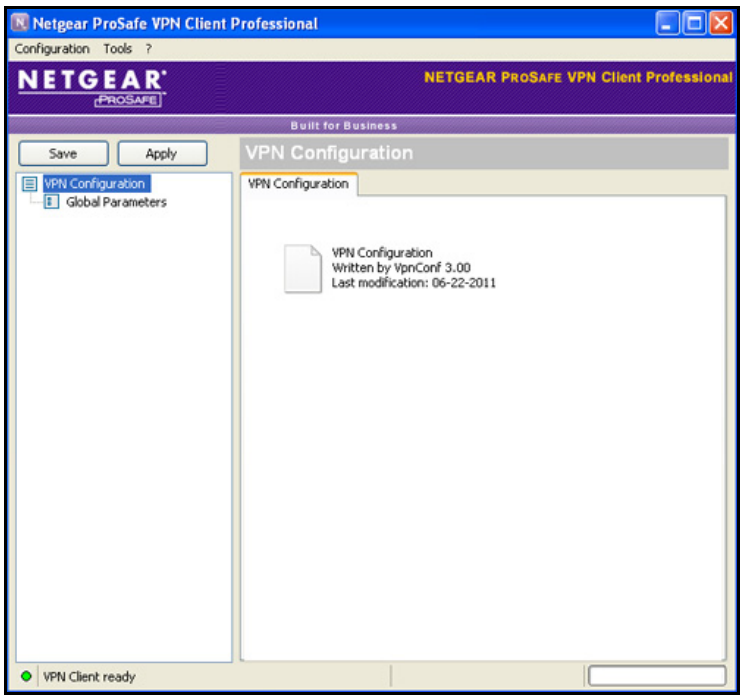


Figure 96.

2. In the tree list pane of the Configuration Panel screen, right-click **VPN Configuratio**n, and select **New Phase 1**.

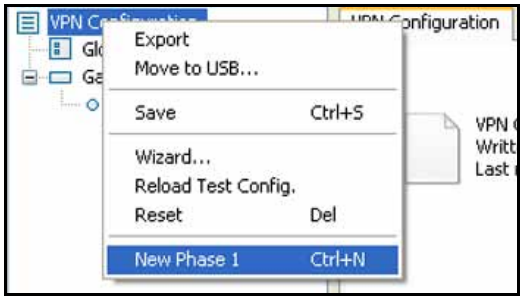


Figure 97.

3. Change the name of the authentication phase (the default is Gateway):
   a. Right-click the authentication phase name.
   b. Select **Rename**.
   c. Type **vpn_client**.
   d. Click anywhere in the tree list pane.

Note: This is the name for the authentication phase that is used only for the VPN client, not during IKE negotiation. You can view and change this name in the tree list pane. This name needs to be a unique name.

The Authentication pane displays in the Configuration Panel screen, with the Authentication tab selected by default.

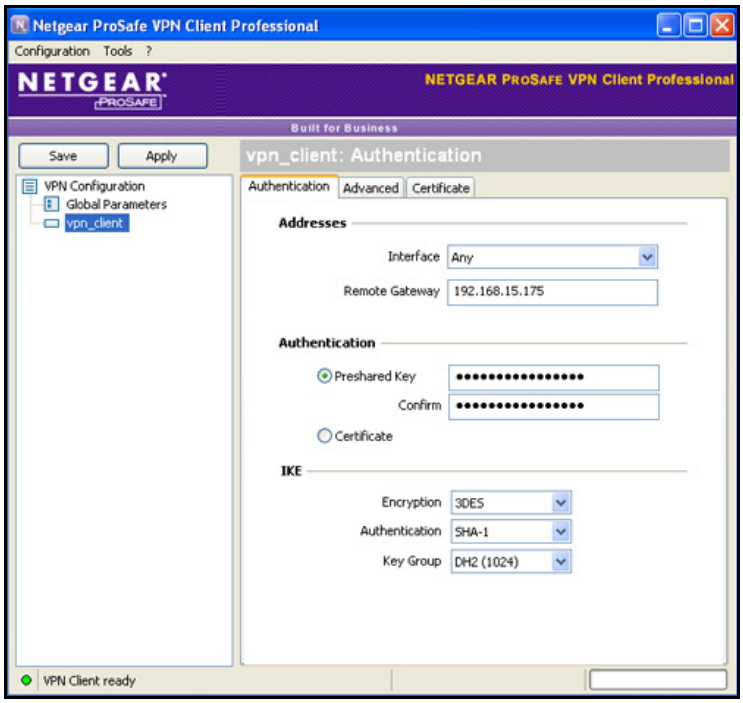


Figure 98.

4. Specify the settings that are explained in the following table.

Table 39. VPN client authentication settings

Setting	Description	
Interface	Select **Any** from the drop-down list.	
Remote Gateway	Enter the remote IP address or DNS name of the wireless VPN firewall. For example, enter **192.168.15.175**.	
Preshared Key	Select the **Preshared Key** radio button. Enter the pre-shared key that you already specified on the wireless VPN firewall. For example, enter **I7!KL39dFG_8**. Confirm the key in the Confirm field.	
IKE	Encryption	Select the **3DES** encryption algorithm from the drop-down list.
	Authentication	Select the **SHA1** authentication algorithm from the drop-down list.
	Key Group	Select the **DH2 (1024)** key group from the drop-down list. **Note:** On the wireless VPN firewall, this key group is referred to as Diffie-Hellman Group 2 (1024 bit).

5. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.
6. Click the **Advanced** tab in the Authentication pane. The Advanced pane displays.

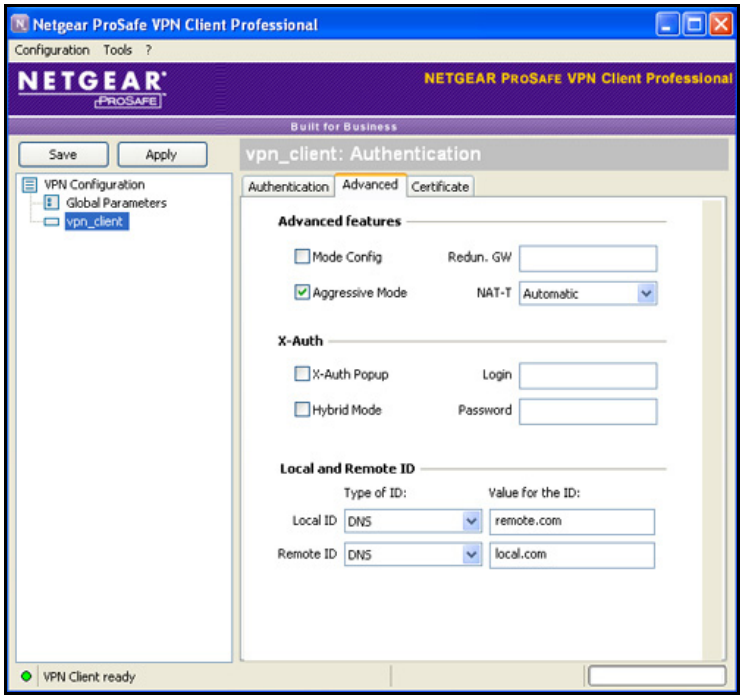


Figure 99.

7. Specify the settings that are explained in the following table.

Table 40. VPN client advanced authentication settings

Setting	Description
Advanced features	
Aggressive Mode	Select this check box to enable aggressive mode as the mode of negotiation with the wireless VPN firewall.
NAT-T	Select **Automatic** from the drop-down list to enable the VPN client and wireless VPN firewall to negotiate NAT-T.
Local and Remote ID	
Local ID	As the type of ID, select **DNS** from the Local ID drop-down list because you specified FQDN in the wireless VPN firewall configuration. As the value of the ID, enter **remote.com** as the local ID for the VPN client. **Note:** The remote ID on the wireless VPN firewall is the local ID on the VPN client. It might be less confusing to configure an FQDN such as client.com as the remote ID on the wireless VPN firewall and then enter client.com as the local ID on the VPN client.

Table 40. VPN client advanced authentication settings (continued)

Setting	Description
Remote ID	As the type of ID, select **DNS** from the Remote ID drop-down list because you specified an FQDN in the wireless VPN firewall configuration. As the value of the ID, enter **local.com** as the remote ID for the wireless VPN firewall. **Note:** The local ID on the wireless VPN firewall is the remote ID on the VPN client. It might be less confusing to configure an FQDN such as router.com as the local ID on the wireless VPN firewall and then enter router.com as the remote ID on the VPN client.

8. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.

Create the IPSec Configuration (Phase 2 Settings)

Note: On the wireless VPN firewall, the IPSec configuration (phase 2 settings) is referred to as the IKE settings.

➢ **To create an IPSec configuration:**

1. In the tree list pane of the Configuration Panel screen, right-click the **vpn_client** authentication phase name, and then select **New Phase 2**.
2. Change the name of the IPSec configuration (the default is Tunnel):
   a. Right-click the IPSec configuration name.
   b. Select **Rename**.
   c. Type **netgear_platform**.
   d. Click anywhere in the tree list pane.

   Note: *This is the name for the IPSec configuration that is used only for the VPN client, not during IPSec negotiation. You can view and change this name in the tree list pane. This name needs to be a unique name.*

   The IPSec pane displays in the Configuration Panel screen, with the IPSec tab selected by default.

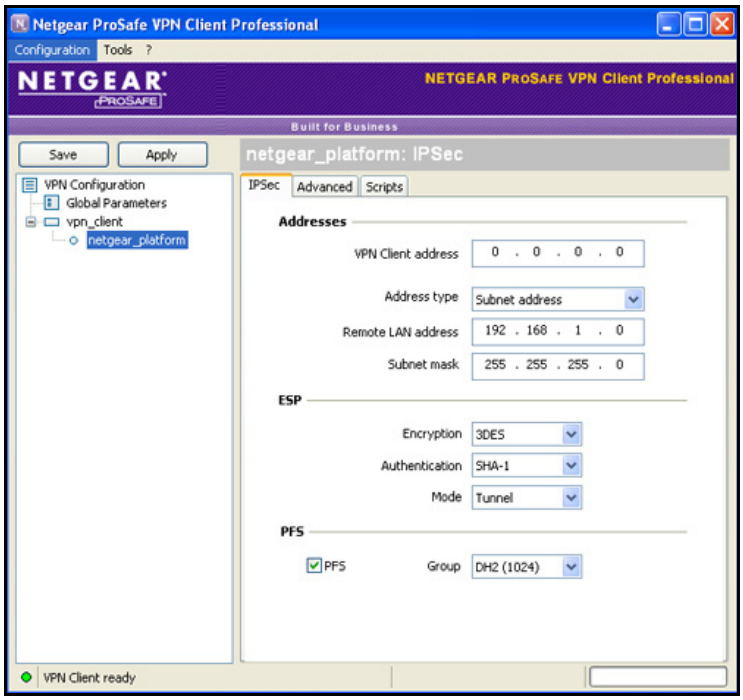


Figure 100.

3. Specify the settings that are explained in the following table.

Table 41. VPN client IPSec configuration settings

Setting	Description	
VPN Client address	Either enter **0.0.0.0** as the IP address, or enter a virtual IP address that is used by the VPN client in the wireless VPN firewall's LAN; the computer (for which the VPN client opened a tunnel) appears in the LAN with this IP address.	
Address Type	Select **Subnet address** from the drop-down list. This selection defines which addresses the VPN client can communicate with after the VPN tunnel is established.	
Remote LAN address	Enter **192.168.1.0** as the remote IP address (that is, LAN network address) of the gateway that opens the VPN tunnel.	
Subnet mask	Enter **255.255.255.0** as the remote subnet mask of the gateway that opens the VPN tunnel.	
ESP	Encryption	Select **3DES** as the encryption algorithm from the drop-down list.
	Authentication	Select **SHA-1** as the authentication algorithm from the drop-down list.
	Mode	Select **Tunnel** as the encapsulation mode from the drop-down list.
PFS and Group	Select the **PFS** check box, and then select the **DH2 (1024)** key group from the drop-down list. **Note:** On the wireless VPN firewall, this key group is referred to as Diffie-Hellman Group 2 (1024 bit).	

4. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.

Configure the Global Parameters

➢ **To specify the global parameters:**

1. Click **Global Parameters** in the left column of the Configuration Panel screen. The Global Parameters pane displays in the Configuration Panel screen.

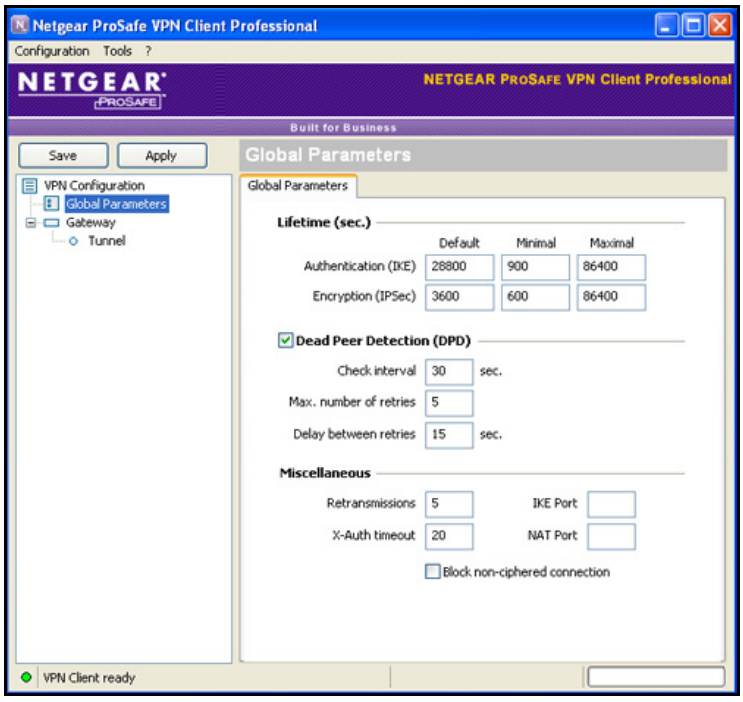


Figure 101.

2. Specify the default lifetimes in seconds:
   - **Authentication (IKE)**, **Default**. The default lifetime value is 3600 seconds. Change this setting to **28800** seconds to match the configuration of the wireless VPN firewall.
   - **Encryption (IPSec)**, **Default**. The default lifetime value is 1200 seconds. Change this setting to **3600** seconds to match the configuration of the wireless VPN firewall.
3. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.

The wireless VPN firewall configuration is now complete.

Test the Connection and View Connection and Status Information

Both the NETGEAR ProSafe VPN Client and the wireless VPN firewall provide VPN connection and status information. This information is useful for verifying the status of a connection and troubleshooting problems with a connection.

Test the NETGEAR VPN Client Connection

There are many ways to establish a connection. The following procedures assume that you use the default authentication phase name *Gateway* and the default IPSec configuration name *Tunnel*. If you manually set up the connection and changed the names, use *vpn_client* (or any other name that you have configured) as the authentication phase name and *netgear_platform* (or any other name that you have configured) as the IPSec configuration name.

➢ **To establish a connection, use one of the following three methods:**

- **Use the Configuration Panel screen**. In the tree list pane of the Configuration Panel screen, perform *one* of the following tasks:
  - Click the **Tunnel** IPSec configuration name, and press **Ctrl+O.**
  - Right-click the **Tunnel** IPSec configuration name, and select **Open tunnel**.

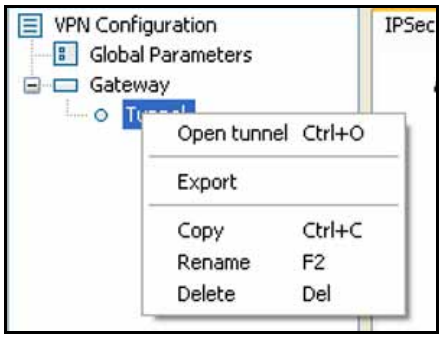


Figure 102.

- **Use the Connection Panel screen**. On the main menu of the Configuration Panel screen, select **Tools > Connection Panel** to open the Connection Panel screen. Perform *one* of the following tasks:
  - Double-click **Gateway-Tunnel**.
  - Right-click **Gateway-Tunnel**, and select **Open tunnel**.
  - Click **Gateway-Tunnel**, and press **Ctrl+O**.

Figure 103.

- **Use the system-tray icon**. Right-click the system tray icon, and select **Open tunnel 'Tunnel'**.

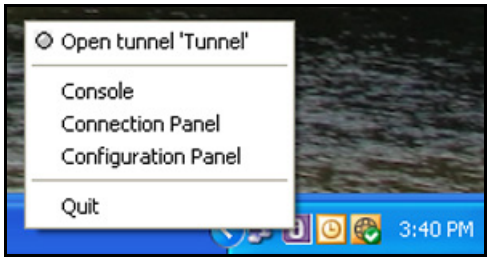


Figure 104.

Whichever way you choose to open the tunnel, when the tunnel opens successfully, the *Tunnel opened* message displays above the system tray:

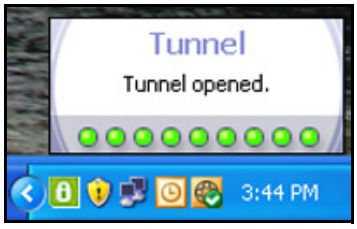


Figure 105.

Once launched, the VPN client displays an icon in the system tray that indicates whether or not a tunnel is opened, using a color code:

Green icon:
at least one VPN tunnel opened

Purple icon:
no VPN tunnel opened

Figure 106.

NETGEAR VPN Client Status and Log Information

➢ **To view detailed negotiation and error information on the NETGEAR VPN client:**

Right-click the VPN client icon in the system tray, and select **Console**. The VPN Client Console Active screen displays.

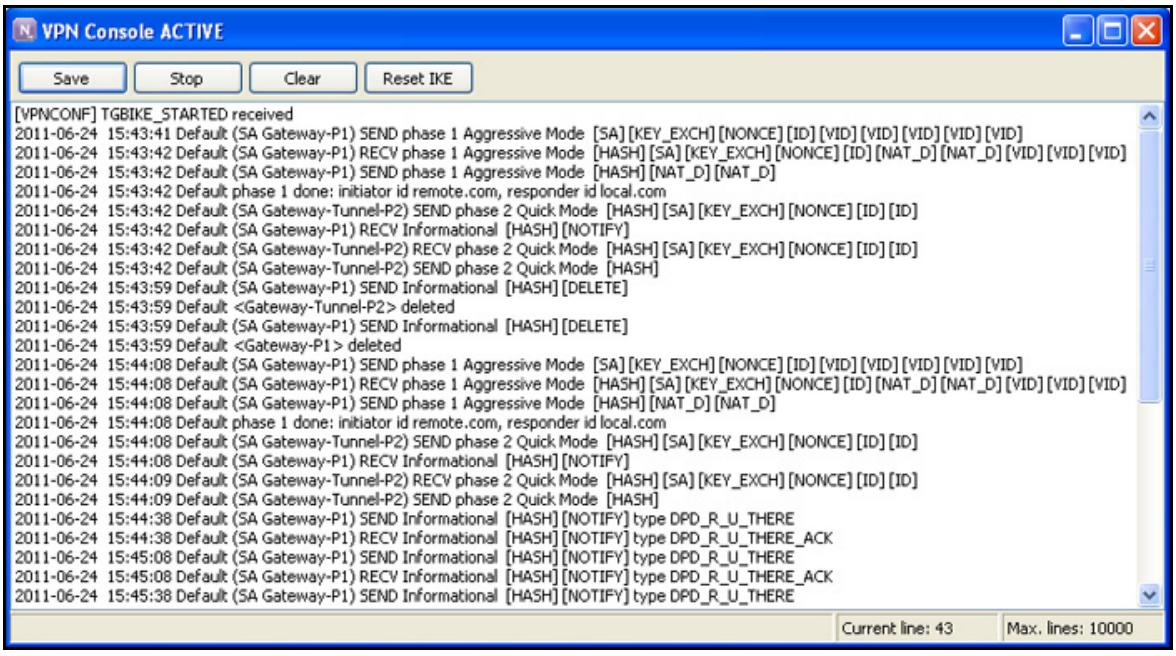

VPN Console ACTIVE
Save
Stop
Clear
Reset IKE
[VPNCONF] TGBIKE_STARTED received
2011-06-24 15:43:41 Default (SA Gateway-P1) SEND phase 1 Aggressive Mode [SA] [KEY_EXCH] [NONCE] [ID] [VID] [VID] [VID] [VID] [VID]
2011-06-24 15:43:42 Default (SA Gateway-P1) RECV phase 1 Aggressive Mode [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [NAT_D] [NAT_D] [VID] [VID] [VID]
2011-06-24 15:43:42 Default (SA Gateway-P1) SEND phase 1 Aggressive Mode [HASH] [NAT_D] [NAT_D]
2011-06-24 15:43:42 Default phase 1 done: initiator id remote.com, responder id local.com
2011-06-24 15:43:42 Default (SA Gateway-Tunnel-P2) SEND phase 2 Quick Mode [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID]
2011-06-24 15:43:42 Default (SA Gateway-P1) RECV Informational [HASH] [NOTIFY]
2011-06-24 15:43:42 Default (SA Gateway-Tunnel-P2) RECV phase 2 Quick Mode [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID]
2011-06-24 15:43:42 Default (SA Gateway-Tunnel-P2) SEND phase 2 Quick Mode [HASH]
2011-06-24 15:43:59 Default (SA Gateway-P1) SEND Informational [HASH] [DELETE]
2011-06-24 15:43:59 Default <Gateway-Tunnel-P2> deleted
2011-06-24 15:43:59 Default (SA Gateway-P1) SEND Informational [HASH] [DELETE]
2011-06-24 15:43:59 Default <Gateway-P1> deleted
2011-06-24 15:44:08 Default (SA Gateway-P1) SEND phase 1 Aggressive Mode [SA] [KEY_EXCH] [NONCE] [ID] [VID] [VID] [VID] [VID] [VID]
2011-06-24 15:44:08 Default (SA Gateway-P1) RECV phase 1 Aggressive Mode [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [NAT_D] [NAT_D] [VID] [VID] [VID]
2011-06-24 15:44:08 Default (SA Gateway-P1) SEND phase 1 Aggressive Mode [HASH] [NAT_D] [NAT_D]
2011-06-24 15:44:08 Default phase 1 done: initiator id remote.com, responder id local.com
2011-06-24 15:44:08 Default (SA Gateway-Tunnel-P2) SEND phase 2 Quick Mode [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID]
2011-06-24 15:44:08 Default (SA Gateway-P1) RECV Informational [HASH] [NOTIFY]
2011-06-24 15:44:09 Default (SA Gateway-Tunnel-P2) RECV phase 2 Quick Mode [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID]
2011-06-24 15:44:09 Default (SA Gateway-Tunnel-P2) SEND phase 2 Quick Mode [HASH]
2011-06-24 15:44:38 Default (SA Gateway-P1) SEND Informational [HASH] [NOTIFY] type DPD_R_U_THERE
2011-06-24 15:44:38 Default (SA Gateway-P1) RECV Informational [HASH] [NOTIFY] type DPD_R_U_THERE_ACK
2011-06-24 15:45:08 Default (SA Gateway-P1) SEND Informational [HASH] [NOTIFY] type DPD_R_U_THERE
2011-06-24 15:45:08 Default (SA Gateway-P1) RECV Informational [HASH] [NOTIFY] type DPD_R_U_THERE_ACK
2011-06-24 15:45:38 Default (SA Gateway-P1) SEND Informational [HASH] [NOTIFY] type DPD_R_U_THERE
Current line: 43
Max. lines: 10000

Figure 107.

View the Wireless VPN Firewall IPSec VPN Connection Status

To review the status of current IPSec VPN tunnels, select **VPN > Connection Status > IPSec VPN Connection Status**. The IPSec VPN Connection Status screen displays. (The following figure shows an IPSec SA as an example.)

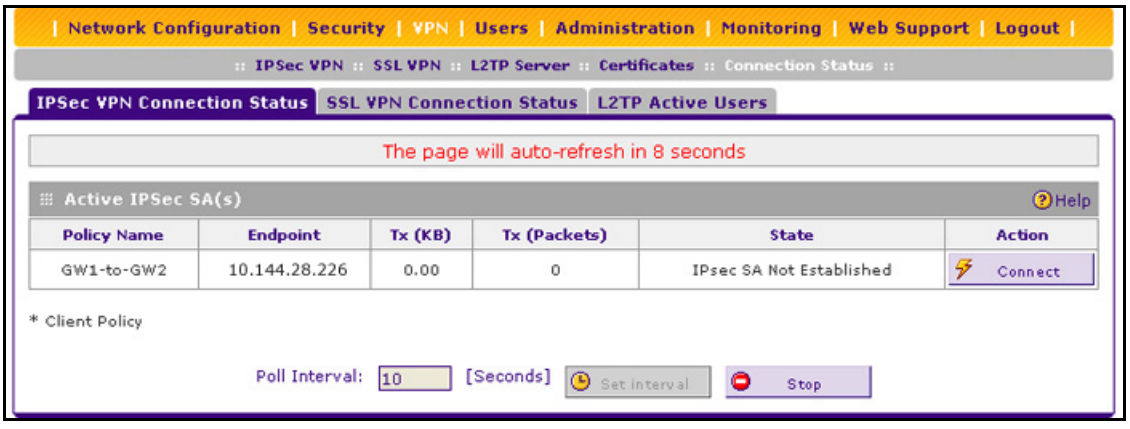


Figure 108.

The Active IPSec SA(s) table lists each active connection with the information that is described in the following table. The default poll interval is 5 seconds. To change the poll

interval period, enter a new value in the Poll Interval field, and then click the **Set Interval** button. To stop polling, click the **Stop** button.

Table 42. IPSec VPN Connection Status screen information

Item	Description
Policy Name	The name of the VPN policy that is associated with this SA.
Endpoint	The IP address on the remote VPN endpoint.
Tx (KB)	The amount of data that is transmitted over this SA.
Tx (Packets)	The number of IP packets that are transmitted over this SA.
State	The current status of the SA. Phase 1 is the authentication phase, and Phase 2 is key exchange phase. If there is no connection, the status is IPSec SA Not Established.
Action	Click the **Connect** table button to build the connection, or click the **Disconnect** table button to terminate the connection.

View the Wireless VPN Firewall IPSec VPN Log

➤ **To display the IPSec VPN log:**

Select **Monitoring > VPN Logs > IPSec VPN Logs.** The IPSec VPN Logs screen displays.

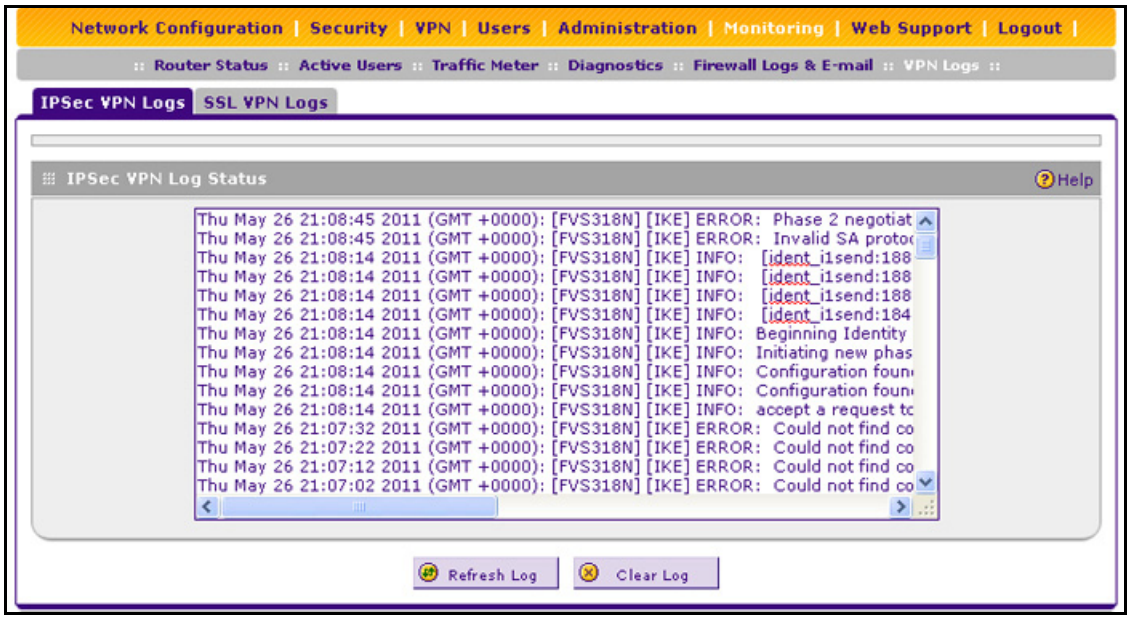

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Router Status :: Active Users :: Traffic Meter :: Diagnostics :: Firewall Logs & E-mail :: VPN Logs ::
IPSec VPN Logs
SSL VPN Logs
IPSec VPN Log Status
Help
Thu May 26 21:08:45 2011 (GMT +0000): [FVS318N] [IKE] ERROR: Phase 2 negotiat
Thu May 26 21:08:45 2011 (GMT +0000): [FVS318N] [IKE] ERROR: Invalid SA protoc
Thu May 26 21:08:14 2011 (GMT +0000): [FVS318N] [IKE] INFO: [ident_i1send:188
Thu May 26 21:08:14 2011 (GMT +0000): [FVS318N] [IKE] INFO: [ident_i1send:188
Thu May 26 21:08:14 2011 (GMT +0000): [FVS318N] [IKE] INFO: [ident_i1send:188
Thu May 26 21:08:14 2011 (GMT +0000): [FVS318N] [IKE] INFO: [ident_i1send:184
Thu May 26 21:08:14 2011 (GMT +0000): [FVS318N] [IKE] INFO: Beginning Identity
Thu May 26 21:08:14 2011 (GMT +0000): [FVS318N] [IKE] INFO: Initiating new phas
Thu May 26 21:08:14 2011 (GMT +0000): [FVS318N] [IKE] INFO: Configuration foun
Thu May 26 21:08:14 2011 (GMT +0000): [FVS318N] [IKE] INFO: Configuration foun
Thu May 26 21:08:14 2011 (GMT +0000): [FVS318N] [IKE] INFO: accept a request tc
Thu May 26 21:07:32 2011 (GMT +0000): [FVS318N] [IKE] ERROR: Could not find co
Thu May 26 21:07:22 2011 (GMT +0000): [FVS318N] [IKE] ERROR: Could not find co
Thu May 26 21:07:12 2011 (GMT +0000): [FVS318N] [IKE] ERROR: Could not find co
Thu May 26 21:07:02 2011 (GMT +0000): [FVS318N] [IKE] ERROR: Could not find co
Refresh Log
Clear Log

Figure 109.

Manage IPSec VPN Policies

After you have used the VPN Wizard to set up a VPN tunnel, a VPN policy and an IKE policy are stored in separate policy tables. The name that you selected as the VPN tunnel connection name during the VPN Wizard setup identifies both the VPN policy and IKE policy. You can edit existing policies, or manually add new VPN and IKE policies directly in the policy tables.

Manage IKE Policies

The Internet Key Exchange (IKE) protocol performs negotiations between the two VPN gateways and provides automatic management of the keys that are used for IPSec connections. It is important to remember that:

- An automatically generated VPN policy (auto policy) needs to use the IKE negotiation protocol.
- A manually generated VPN policy (manual policy) cannot use the IKE negotiation protocol.

IKE policies are activated when the following situations occur:

1. The VPN policy selector determines that some traffic matches an existing VPN policy:
   - If the VPN policy is of an auto policy type, the IKE policy that is specified in the Auto Policy Parameters section of the Add VPN Policy screen (see *Figure 113* on page 190) is used to start negotiations with the remote VPN gateway.
   - If the VPN policy is of a manual policy type, the settings that are specified in the Manual Policy Parameters section of the Add VPN Policy screen (see *Figure 113* on page 190) are accessed, and the first matching IKE policy is used to start negotiations with the remote VPN gateway:
     - If negotiations fail, the next matching IKE policy is used.
     - If none of the matching IKE policies are acceptable to the remote VPN gateway, then a VPN tunnel cannot be established.
2. An IKE session is established, using the security association (SA) settings that are specified in a matching IKE policy:
   - Keys and other settings are exchanged.
   - An IPSec SA is established, using the settings that are specified in the VPN policy.

The VPN tunnel is then available for data transfer.

When you use the VPN Wizard to set up a VPN tunnel, an IKE policy is established and populated in the List of IKE Policies, and is given the same name as the new VPN connection name. You can also edit exiting policies or add new IKE policies from the IKE Policies screen.

IKE Policies Screen

➤ **To access the IKE Policies screen:**

Select **VPN > IPSec VPN**. The IPSec VPN submenu tabs display with the IKE Policies screen in view. (The following figure shows some examples.)

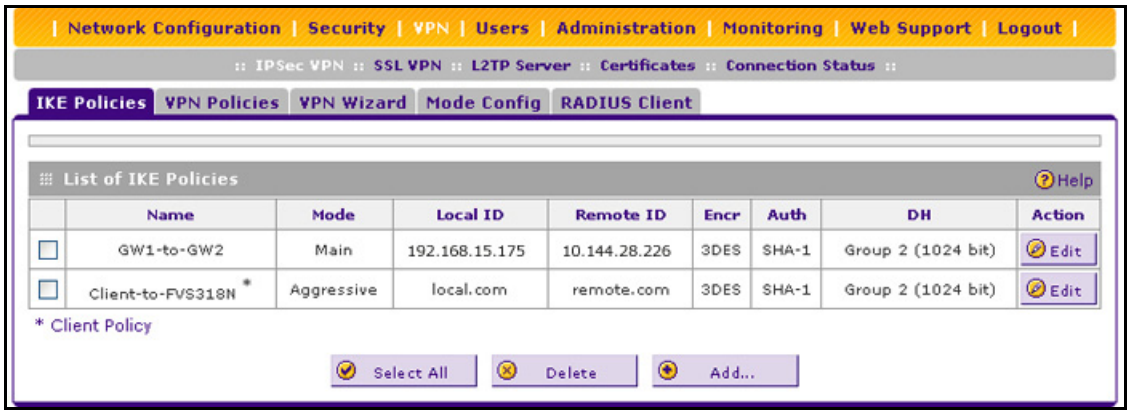


Figure 110.

Each policy contains the data that are explained in the following table. These fields are explained in more detail in *Table 44* on page 183.

Table 43. IKE Policies screen information

Item	Description
Name	The name that identifies the IKE policy. When you use the VPN Wizard to set up a VPN policy, an accompanying IKE policy is automatically created with the same name that you select for the VPN policy. **Note:** The name is not supplied to the remote VPN endpoint.
Mode	The exchange mode: Main or Aggressive.
Local ID	The IKE/ISAKMP identifier of the wireless VPN firewall. The remote endpoint needs to have this value as its remote ID.
Remote ID	The IKE/ISAKMP identifier of the remote endpoint, which needs to have this value as its local ID.
Encr	The encryption algorithm that is used for the IKE security association (SA). This setting needs to match the setting on the remote endpoint.
Auth	The authentication algorithm that is used for the IKE SA. This setting needs to match the setting on the remote endpoint.
DH	The Diffie-Hellman (DH) group that is used when keys are exchanged. This setting needs to match the setting on the remote endpoint.

➢ **To delete one or more IKE polices:**

1. Select the check box to the left of each policy that you want to delete, or click the **Select All** table button to select all IKE policies.
2. Click the **Delete** table button.

For information about how to add or edit an IKE policy, see *Manually Add or Edit an IKE Policy* on page 181.

Note: You cannot delete or edit an IKE policy for which the VPN policy is active without first disabling or deleting the VPN policy.

Manually Add or Edit an IKE Policy

➢ **To manually add an IKE policy:**

1. Select **VPN > IPSec VPN**. The IPSec VPN submenu tabs display with the IKE Policies screen in view (see the previous figure).
2. Under the List of IKE Policies table, click the **Add** table button. The Add IKE Policy screen displays:

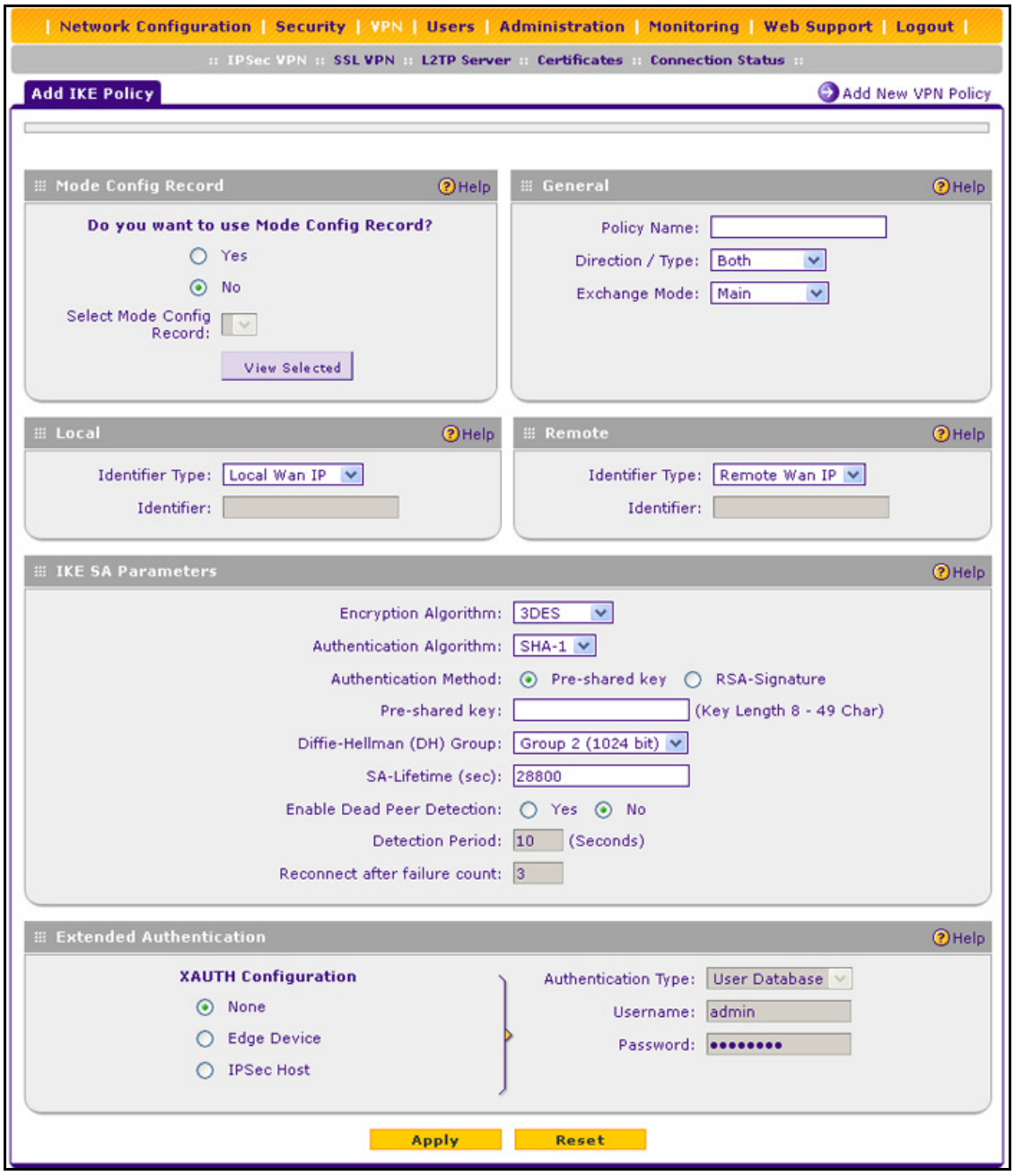

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
IPSec VPN :: SSL VPN :: L2TP Server :: Certificates :: Connection Status
Add IKE Policy
Add New VPN Policy
Mode Config Record
Help
Do you want to use Mode Config Record?
Yes
No
Select Mode Config Record:
View Selected
General
Help
Policy Name:
Direction / Type: Both
Exchange Mode: Main
Local
Help
Identifier Type: Local Wan IP
Identifier:
Remote
Help
Identifier Type: Remote Wan IP
Identifier:
IKE SA Parameters
Help
Encryption Algorithm: 3DES
Authentication Algorithm: SHA-1
Authentication Method: Pre-shared key RSA-Signature
Pre-shared key: (Key Length 8 - 49 Char)
Diffie-Hellman (DH) Group: Group 2 (1024 bit)
SA-Lifetime (sec): 28800
Enable Dead Peer Detection: Yes No
Detection Period: 10 (Seconds)
Reconnect after failure count: 3
Extended Authentication
Help
XAUTH Configuration
None
Edge Device
IPSec Host
Authentication Type: User Database
Username: admin
Password: ••••••••
Apply
Reset

Figure 111.

3. Complete the settings as explained in the following table:

Table 44. Add IKE Policy screen settings

Setting	Description	
Mode Config Record		
Do you want to use Mode Config Record?	Specify whether or not the IKE policy uses a Mode Config record. For information about how to define a Mode Config record, see *Mode Config Operation* on page 199. Select one of the following radio buttons: • **Yes**. IP addresses are assigned to remote VPN clients. You need to select a Mode Config record from the drop-down list. Because Mode Config functions only in Aggressive mode, selecting the Yes radio button sets the tunnel exchange mode to Aggressive mode and disables the Main mode. Mode Config also requires that both the local and remote endpoints are defined by their FQDNs. • **No**. Disables Mode Config for this IKE policy.	
	Select Mode Config Record	From the drop-down list, select one of the Mode Config records that you defined on the Add Mode Config Record screen (see *Configure Mode Config Operation on the Wireless VPN Firewall* on page 199). **Note:** Click the **View Selected** button to open the Selected Mode Config Record Details pop-up screen.
General		
Policy Name	A descriptive name of the IKE policy for identification and management purposes. **Note:** The name is not supplied to the remote VPN endpoint.	
Direction / Type	From the drop-down list, select the connection method for the wireless VPN firewall: • **Initiator**. The wireless VPN firewall initiates the connection to the remote endpoint. • **Responder**. The wireless VPN firewall responds only to an IKE request from the remote endpoint. • **Both**. The wireless VPN firewall can both initiate a connection to the remote endpoint and respond to an IKE request from the remote endpoint.	
Exchange Mode	From the drop-down list, select the mode of exchange between the wireless VPN firewall and the remote VPN endpoint: • **Main**. This mode is slower than the Aggressive mode but more secure. • **Aggressive**. This mode is faster than the Main mode but less secure. **Note:** If you specify either an FQDN or a user FQDN name as the local ID or remote ID (see the Identifier sections later in this table), the Aggressive mode is automatically selected.	

Table 44. Add IKE Policy screen settings (continued)

Setting	Description	
Local		
Identifier	From the drop-down list, select one of the following ISAKMP identifiers to be used by the wireless VPN firewall, and then specify the identifier in the Identifier field: • **Local Wan IP**. The WAN IP address of the wireless VPN firewall. When you select this option, the Identifier field automatically shows the IP address of the selected WAN interface. • **FQDN**. The Internet address for the wireless VPN firewall. • **User FQDN**. The email address for a local VPN client or the wireless VPN firewall. • **DER ASN1 DN**. A distinguished name (DN) that identifies the wireless VPN firewall in the DER encoding and ASN.1 format.	
	Identifier	Depending on the selection of the Identifier drop-down list, enter the IP address, email address, FQDN, or distinguished name.
Remote		
Identifier	From the drop-down list, select one of the following ISAKMP identifiers to be used by the remote endpoint, and then specify the identifier in the Identifier field: • **Remote Wan IP**. The WAN IP address of the remote endpoint. When you select this option, the Identifier field automatically shows the IP address of the selected WAN interface. • **FQDN**. The FQDN for a remote gateway. • **User FQDN**. The email address for a remote VPN client or gateway. • **DER ASN1 DN**. A distinguished name (DN) that identifies the remote endpoint in the DER encoding and ASN.1 format.	
	Identifier	Depending on the selection of the Identifier drop-down list, enter the IP address, email address, FQDN, or distinguished name.
IKE SA Parameters		
Encryption Algorithm	From the drop-down list, select one of the following five algorithms to negotiate the security association (SA): • **DES**. Data Encryption Standard (DES). • **3DES**. Triple DES. This is the default algorithm. • **AES-128**. Advanced Encryption Standard (AES) with a 128-bit key size. • **AES-192**. AES with a 192-bit key size. • **AES-256**. AES with a 256-bit key size.	
Authentication Algorithm	From the drop-down list, select one of the following two algorithms to use in the VPN header for the authentication process: • **SHA-1**. Hash algorithm that produces a 160-bit digest. This is the default setting. • **MD5**. Hash algorithm that produces a 128-bit digest.	

Table 44. Add IKE Policy screen settings (continued)

Setting	Description	
Authentication Method	Select one of the following radio buttons to specify the authentication method: • **Pre-shared key**. A secret that is shared between the wireless VPN firewall and the remote endpoint. • **RSA-Signature**. Uses the active self-signed certificate that you uploaded on the Certificates screen (see *Manage VPN Self-Signed Certificates* on page 265). The pre-shared key is masked out when you select RSA-Signature.	
	Pre-shared key	A key with a minimum length of 8 characters and no more than 49 characters. Do not use a double quote (“) in the key.
Diffie-Hellman (DH) Group	The DH Group sets the strength of the algorithm in bits. The higher the group, the more secure the exchange. From the drop-down list, select one of the following three strengths: • **Group 1 (768 bit)**. • **Group 2 (1024 bit)**. This is the default setting. • **Group 5 (1536 bit)**. **Note:** Ensure that the DH Group is configured identically on both sides.	
SA-Lifetime (sec)	The period in seconds for which the IKE SA is valid. When the period times out, the next rekeying occurs. The default is 28800 seconds (8 hours).	
Enable Dead Peer Detection **Note:** See also *Configure Keep-Alives and Dead Peer Detection* on page 215.	Select a radio button to specify whether or not Dead Peer Detection (DPD) is enabled: • **Yes**. This feature is enabled. When the wireless VPN firewall detects an IKE connection failure, it deletes the IPSec and IKE SA and forces a reestablishment of the connection. You need to specify the detection period in the Detection Period field and the maximum number of times that the wireless VPN firewall attempts to reconnect in the Reconnect after failure count field. • **No**. This feature is disabled. This is the default setting.	
	Detection Period	The period in seconds between consecutive DPD R-U-THERE messages, which are sent only when the IPSec traffic is idle.
	Reconnect after failure count	The maximum number of DPD failures before the wireless VPN firewall tears down the connection and then attempts to reconnect to the peer. The default is 3 failures.

Table 44. Add IKE Policy screen settings (continued)

Setting	Description	
Extended Authentication		
XAUTH Configuration **Note:** For more information about XAUTH and its authentication modes, see *Configure XAUTH for VPN Clients* on page 195.	Select one of the following radio buttons to specify whether or not Extended Authentication (XAUTH) is enabled, and, if enabled, which device is used to verify user account information: • **None**. XAUTH is disabled. This the default setting. • **Edge Device**. The wireless VPN firewall functions as a VPN concentrator on which one or more gateway tunnels terminate. The authentication modes that are available for this configuration are User Database, RADIUS PAP, or RADIUS CHAP. • **IPSec Host**. The wireless VPN firewall functions as a VPN client of the remote gateway. In this configuration the wireless VPN firewall is authenticated by a remote gateway with a user name and password combination.	
	Authentication Type	For an Edge Device configuration, from the drop-down list, select one of the following authentication types: • **User Database**. XAUTH occurs through the wireless VPN firewall's user database. You can add users on the Add User screen (see *User Database Configuration* on page 196). • **Radius PAP**. XAUTH occurs through RADIUS Password Authentication Protocol (PAP). The local user database is first checked. If the user account is not present in the local user database, the wireless VPN firewall connects to a RADIUS server. For more information, see *RADIUS Client Configuration* on page 196. • **Radius CHAP**. XAUTH occurs through RADIUS Challenge Handshake Authentication Protocol (CHAP). For more information, see *RADIUS Client Configuration* on page 196.
	Username	The user name for XAUTH.
	Password	The password for XAUTH.

4. Click **Apply** to save your settings. The IKE policy is added to the List of IKE Policies table.

➢ **To edit an IKE policy:**

1. Select **VPN > IPSec VPN**. The IPSec VPN submenu tabs display with the IKE Policies screen in view (see *Figure 110* on page 180).
2. In the List of IKE Policies table, click the **Edit** table button to the right of the IKE policy that you want to edit. The Edit IKE Policy screen displays. This screen shows the same fields as the Add IKE Policy screen (see *Figure 111* on page 182).
3. Modify the settings that you wish to change (see the previous table).
4. Click **Apply** to save your changes. The modified IKE policy is displayed in the List of IKE Policies table.

Manage VPN Policies

You can create two types of VPN policies. When you use the VPN Wizard to create a VPN policy, only the Auto method is available.

- **Manual**. You manually enter all settings (including the keys) for the VPN tunnel on the wireless VPN firewall and on the remote VPN endpoint. No third-party server or organization is involved.
- **Auto**. Some settings for the VPN tunnel are generated automatically through the use of the IKE (Internet Key Exchange) Protocol to perform negotiations between the two VPN endpoints (the local ID endpoint and the remote ID endpoint). You still need to manually enter all settings on the remote VPN endpoint (unless the remote VPN endpoint also has a VPN Wizard).

In addition, a certification authority (CA) can also be used to perform authentication (see *Manage Digital Certificates for VPN Connections* on page 262). For gateways to use a CA to perform authentication, each VPN gateway needs to have a certificate from the CA. For each certificate, there is both a public key and a private key. The public key is freely distributed, and is used by any sender to encrypt data intended for the receiver (the key owner). The receiver then uses its private key to decrypt the data (without the private key, decryption is impossible). The use of certificates for authentication reduces the amount of data entry that is required on each VPN endpoint.

VPN Policies Screen

The VPN Policies screen allows you to add additional policies—either Auto or Manual—and to manage the VPN policies already created. You can edit policies, enable or disable policies, or delete them entirely. These are the rules for VPN policy use:

- Traffic covered by a policy is automatically sent through a VPN tunnel.
- When traffic is covered by two or more policies, the first matching policy is used. (In this situation, the order of the policies is important. However, if you have only one policy for each remote VPN endpoint, then the policy order is not important.)
- The VPN tunnel is created according to the settings in the security association (SA).
- The remote VPN endpoint needs to have a matching SA; otherwise, it refuses the connection.

To access the VPN Policies screen, select **VPN > IPSec VPN > VPN Policies**. The VPN Policies screen displays. (The following figure shows some examples.)

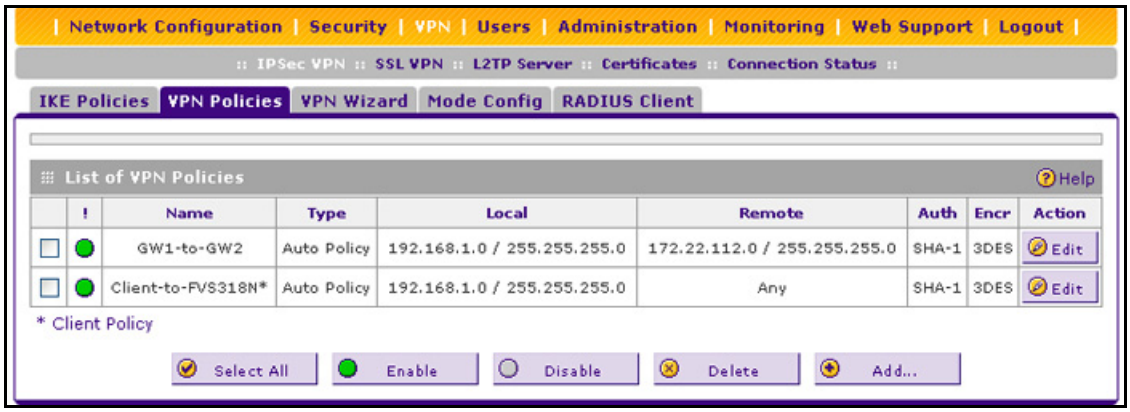

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
IPSec VPN :: SSL VPN :: L2TP Server :: Certificates :: Connection Status
IKE Policies | VPN Policies | VPN Wizard | Mode Config | RADIUS Client
List of VPN Policies
Help
! Name Type Local Remote Auth Encr Action
GW1-to-GW2 Auto Policy 192.168.1.0 / 255.255.255.0 172.22.112.0 / 255.255.255.0 SHA-1 3DES Edit
Client-to-FVS318N* Auto Policy 192.168.1.0 / 255.255.255.0 Any SHA-1 3DES Edit
* Client Policy
Select All
Enable
Disable
Delete
Add...

Figure 112.

Each policy contains the data that are explained in the following table. These fields are explained in more detail in *Table 46* on page 191.

Table 45. VPN Policies screen information

Item	Description
! (Status)	Indicates whether the policy is enabled (green circle) or disabled (gray circle). To enable or disable a policy, select the check box adjacent to the circle, and click the **Enable** or **Disable** table button, as appropriate.
Name	The name that identifies the VPN policy. When you use the VPN Wizard to create a VPN policy, the name of the VPN policy (and of the automatically created accompanying IKE policy) is the connection name.
Type	Auto or Manual as described previously (Auto is used during VPN Wizard configuration).
Local	IP address (either a single address, range of address, or subnet address) on your LAN. Traffic needs to be from (or to) these addresses to be covered by this policy. (The subnet address is supplied as the default IP address when you are using the VPN Wizard.)
Remote	IP address or address range of the remote network. Traffic needs to be to (or from) these addresses to be covered by this policy. (The VPN Wizard default requires the remote LAN IP address and subnet mask.)
Auth	The authentication algorithm that is used for the VPN tunnel. This setting needs to match the setting on the remote endpoint.
Encr	The encryption algorithm that is used for the VPN tunnel. This setting needs to match the setting on the remote endpoint.

➢ To delete one or more VPN polices:

1. Select the check box to the left of each policy that you want to delete, or click the **Select All** table button to select all VPN policies.
2. Click the **Delete** table button.

➢ **To enable or disable one or more VPN policies:**

1. Select the check box to the left of each policy that you want to enable or disable, or click the **Select All** table button to select all VPN Policies.
2. Click the **Enable** or **Disable** table button.

For information about how to add or edit a VPN policy, see *Manually Add or Edit a VPN Policy* on this page.

Manually Add or Edit a VPN Policy

➢ **To manually add a VPN policy:**

1. Select **VPN > IPSec VPN > VPN Policies**. The VPN Policies screen displays (see *Figure 112* on page 188).
2. Under the List of VPN Policies table, click the **Add** table button. The Add VPN Policy screen displays:

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
IPSec VPN :: SSL VPN :: L2TP Server :: Certificates :: Connection Status ::
Add New VPN Policy
General
Help
Policy Name:
Policy Type: Auto Policy
Remote Endpoint: IP Address:
FQDN:
Enable NetBIOS?
Enable Keepalive: Yes No
Ping IP Address:
Detection Period: 10 (Seconds)
Reconnect after failure count: 3
Traffic Selection
Help
Local IP: Subnet
Start IP:
End IP:
Subnet Mask:
Remote IP: Subnet
Start IP:
End IP:
Subnet Mask:
Manual Policy Parameters
Help
SPI-Incoming: 0x (Hex, 3-8 Chars)
Encryption Algorithm: 3DES
Key-In:
Key-Out:
(DES-8 Char & 3DES-24 Char)
SPI-Outgoing: 0x (Hex, 3-8 Chars)
Integrity Algorithm: SHA-1
Key-In:
Key-Out:
(MD5-16 Char & SHA-1-20 Char)
Auto Policy Parameters
Help
SA Lifetime: 3600 Seconds
Encryption Algorithm: 3DES
Integrity Algorithm: SHA-1
PFS Key Group: DH Group 2 (1024 bit)
Select IKE Policy: GW1-to-GW2 View Selected
Apply
Reset

Figure 113.

3. Complete the settings as explained in the following table:

Table 46. Add New VPN Policy screen settings

Setting	Description	
General		
Policy Name	A descriptive name of the VPN policy for identification and management purposes. **Note:** The name is not supplied to the remote VPN endpoint.	
Policy Type	From the drop-down list, select one of the following policy types: • **Auto Policy**. Some settings (the ones in the Manual Policy Parameters section of the screen) for the VPN tunnel are generated automatically. • **Manual Policy**. All settings need to be specified manually, including the ones in the Manual Policy Parameters section of the screen.	
Remote Endpoint	Select a radio button to specify how the remote endpoint is defined: • **IP Address**. Enter the IP address of the remote endpoint in the fields to the right of the radio button. • **FQDN**. Enter the FQDN of the remote endpoint in the field to the right of the radio button.	
Enable NetBIOS?	Select this check box to allow NetBIOS broadcasts to travel over the VPN tunnel. For more information about NetBIOS, see *Configure NetBIOS Bridging with IPSec VPN* on page 217. This feature is disabled by default.	
Enable Keepalive **Note:** See also *Configure Keep-Alives and Dead Peer Detection* on page 215.	Select a radio button to specify if keep-alive is enabled: • **Yes**. This feature is enabled: Periodically, the wireless VPN firewall sends keep-alive requests (ping packets) to the remote endpoint to keep the tunnel alive. You need to specify the ping IP address in the Ping IP Address field, the detection period in the Detection Period field, and the maximum number of keep-alive requests that the wireless VPN firewall sends in the Reconnect after failure count field. • **No**. This feature is disabled. This is the default setting.	
	Ping IP Address	The IP address that the wireless VPN firewall pings. The address needs to be of a host that can respond to ICMP ping requests.
	Detection Period	The period in seconds between the keep-alive requests. The default setting is 10 seconds.
	Reconnect after failure count	The maximum number of keep-alive requests before the wireless VPN firewall tears down the connection and then attempts to reconnect to the remote endpoint. The default setting is 3 keep-alive requests.

Table 46. Add New VPN Policy screen settings (continued)

Setting	Description
Traffic Selection	
Local IP	From the drop-down list, select the address or addresses that are part of the VPN tunnel on the wireless VPN firewall: • **Any**. All PCs and devices on the network. • **Single**. A single IP address on the network. Enter the IP address in the Start IP Address field. • **Range**. A range of IP addresses on the network. Enter the starting IP address in the Start IP Address field and the ending IP address in the End IP Address field. • **Subnet**. A subnet on the network. Enter the starting IP address in the Start IP Address field and the subnet mask in the Subnet Mask field. **Note:** You cannot select Any for both the wireless VPN firewall and the remote endpoint.
Remote IP	From the drop-down list, select the address or addresses that are part of the VPN tunnel on the remote endpoint. The selections are the same as for the Local IP drop-down list.
Manual Policy Parameters **Note:** These fields apply only when you select Manual Policy as the policy type. When you specify the settings for the fields in this section, a security association (SA) is created.	
SPI-Incoming	The Security Parameters Index (SPI) for the inbound policy. Enter a hexadecimal value between 3 and 8 characters (for example, 0x1234).
Encryption Algorithm	From the drop-down list, select one of the following five algorithms to negotiate the security association (SA): • **3DES**. Triple DES. This is the default algorithm. • **None**. No encryption algorithm. • **DES**. Data Encryption Standard (DES). • **AES-128**. Advanced Encryption Standard (AES) with a 128-bit key size. • **AES-192**. AES with a 192-bit key size. • **AES-256**. AES with a 256-bit key size.
Key-In	The encryption key for the inbound policy. The length of the key depends on the selected encryption algorithm: • **3DES**. Enter 24 characters. • **None**. Key is not applicable. • **DES**. Enter 8 characters. • **AES-128**. Enter 16 characters. • **AES-192**. Enter 24 characters. • **AES-256**. Enter 32 characters.

Table 46. Add New VPN Policy screen settings (continued)

Setting	Description
Key-Out	The encryption key for the outbound policy. The length of the key depends on the selected encryption algorithm: • **3DES**. Enter 24 characters. • **None**. Key is not applicable. • **DES**. Enter 8 characters. • **AES-128**. Enter 16 characters. • **AES-192**. Enter 24 characters. • **AES-256**. Enter 32 characters.
SPI-Outgoing	The Security Parameters Index (SPI) for the outbound policy. Enter a hexadecimal value between 3 and 8 characters (for example, 0x1234).
Integrity Algorithm	From the drop-down list, select one of the following two algorithms to be used in the VPN header for the authentication process: • **SHA-1**. Hash algorithm that produces a 160-bit digest. This is the default setting. • **MD5**. Hash algorithm that produces a 128-bit digest.
Key-In	The integrity key for the inbound policy. The length of the key depends on the selected integrity algorithm: • **MD5**. Enter 16 characters. • **SHA-1**. Enter 20 characters.
Key-Out	The integrity key for the outbound policy. The length of the key depends on the selected integrity algorithm: • **MD5**. Enter 16 characters. • **SHA-1**. Enter 20 characters.
Auto Policy Parameters **Note:** These fields apply only when you select Auto Policy as the policy type.	
SA Lifetime	The lifetime of the security association (SA) is the period or the amount of transmitted data after which the SA becomes invalid and needs to be renegotiated. From the drop-down list, select how the SA lifetime is specified: • **Seconds**. In the SA Lifetime field, enter a period in seconds. The minimum value is 300 seconds. The default setting is 3600 seconds. • **KBytes**. In the SA Lifetime field, enter a number of kilobytes. The minimum value is 1920000 KB.
Encryption Algorithm	From the drop-down list, select one of the following five algorithms to negotiate the security association (SA): • **3DES**. Triple DES. This is the default algorithm. • **None**. No encryption algorithm. • **DES**. Data Encryption Standard (DES). • **AES-128**. Advanced Encryption Standard (AES) with a 128-bit key size. • **AES-192**. AES with a 192-bit key size. • **AES-256**. AES with a 256-bit key size.

Table 46. Add New VPN Policy screen settings (continued)

Setting	Description
Integrity Algorithm	From the drop-down list, select one of the following two algorithms to be used in the VPN header for the authentication process: • **SHA-1**. Hash algorithm that produces a 160-bit digest. This is the default setting. • **MD5**. Hash algorithm that produces a 128-bit digest.
PFS Key Group	Select this check box to enable Perfect Forward Secrecy (PFS), and then select a Diffie-Hellman (DH) group from the drop-down list. The DH Group sets the strength of the algorithm in bits. The higher the group, the more secure the exchange. From the drop-down list, select one of the following three strengths: • **Group 1 (768 bit)**. • **Group 2 (1024 bit)**. This is the default setting. • **Group 5 (1536 bit)**.
Select IKE Policy	Select an existing IKE policy that defines the characteristics of the Phase-1 negotiation. To display the selected IKE policy, click the **View Selected** button.

4. Click **Apply** to save your settings. The VPN policy is added to the List of VPN Policies table.

➢ **To edit a VPN policy:**

1. Select **VPN > IPSec VPN > VPN Policies**. The VPN Policies screen displays (see *Figure 112* on page 188).
2. In the List of VPN Policies table, click the **Edit** table button to the right of the VPN policy that you want to edit. The Edit VPN Policy screen displays. This screen shows the same fields as the Add New VPN Policy screen (see *Figure 113* on page 190).
3. Modify the settings that you wish to change (see the previous table).
4. Click **Apply** to save your changes. The modified VPN policy is displayed in the List of VPN Policies table.

Configure Extended Authentication (XAUTH)

When many VPN clients connect to a wireless VPN firewall, you might want to use a unique user authentication method beyond relying on a single common pre-shared key for all clients. Although you could configure a unique VPN policy for each user, it is more efficient to authenticate users from a stored list of user accounts. XAUTH provides the mechanism for requesting individual authentication information from the user. A local user database or an external authentication server, such as a RADIUS server, provides a method for storing the authentication information centrally in the local network.

You can enable XAUTH when you manually add or edit an IKE policy. Two types of XAUTH are available:

- **Edge Device**. The wireless VPN firewall is used as a VPN concentrator on which one or more gateway tunnels terminate. You need to specify the authentication type that should be used during verification of the credentials of the remote VPN gateways: the user database, RADIUS-PAP, or RADIUS-CHAP.
- **IPSec Host**. Authentication by the remote gateway through a user name and password that are associated with the IKE policy. The user name and password that are used to authenticate the wireless VPN firewall need to be specified on the remote gateway.

Note: If a RADIUS-PAP server is enabled for authentication, XAUTH first checks the local user database for the user credentials. If the user account is not present, the wireless VPN firewall then connects to a RADIUS server.

Configure XAUTH for VPN Clients

Once the XAUTH has been enabled, you need to establish user accounts in the user database to be authenticated against XAUTH, or you need to enable a RADIUS-CHAP or RADIUS-PAP server.

Note: You cannot modify an existing IKE policy to add XAUTH while the IKE policy is in use by a VPN policy. The VPN policy needs to be disabled before you can modify the IKE policy.

➢ **To enable and configure XAUTH:**

1. Select **VPN > IPSec VPN**. The IPSec VPN submenu tabs display with the IKE Policies screen in view (see *Figure 110* on page 180).
2. In the List of IKE Policies table, click the **Edit** table button to the right of the IKE policy for which you want to enable and configure XAUTH. The Edit IKE Policy screen displays. This screen shows the same fields as the Add IKE Policy screen (see *Figure 111* on page 182).
3. In the Extended Authentication section on the screen, complete the settings as explained in the following table:

Table 47. Extended authentication settings

Setting	Description
Select one of the following radio buttons to specify whether or not Extended Authentication (XAUTH) is enabled, and, if enabled, which device is used to verify user account information: • **None**. XAUTH is disabled. This the default setting. • **Edge Device**. The wireless VPN firewall functions as a VPN concentrator on which one or more gateway tunnels terminate. The authentication modes that are available for this configuration are User Database, RADIUS PAP, and RADIUS CHAP. • **IPSec Host**. The wireless VPN firewall functions as a VPN client of the remote gateway. In this configuration the wireless VPN firewall is authenticated by a remote gateway with a user name and password combination.	
Authentication Type	For an Edge Device configuration, from the drop-down list, select one of the following authentication types: • **User Database**. XAUTH occurs through the wireless VPN firewall's user database. You can add users on the Add User screen (see *User Database Configuration* on page 196). • **Radius PAP**. XAUTH occurs through RADIUS Password Authentication Protocol (PAP). The local user database is first checked. If the user account is not present in the local user database, the wireless VPN firewall connects to a RADIUS server. For more information, see *RADIUS Client Configuration* on page 196. • **Radius CHAP**. XAUTH occurs through RADIUS Challenge Handshake Authentication Protocol (CHAP). For more information, see *RADIUS Client Configuration* on page 196.
Username	The user name for XAUTH.
Password	The password for XAUTH.

4. Click **Apply** to save your settings.

User Database Configuration

When XAUTH is enabled in an Edge Device configuration, users need to be authenticated either by a local user database account or by an external RADIUS server. Whether or not you use a RADIUS server, you might want some users to be authenticated locally. These users need to be added to the List of Users table on the Users screen, as described in *Configure User Accounts* on page 254.

RADIUS Client Configuration

Remote Authentication Dial In User Service (RADIUS, RFC 2865) is a protocol for managing authentication, authorization, and accounting (AAA) of multiple users in a network. A RADIUS server stores a database of user information and can validate a user at the request of a gateway or server in the network when a user requests access to network resources. During the establishment of a VPN connection, the VPN gateway can interrupt the process with an XAUTH request. At that point, the remote user needs to provide authentication information such as a user name and password or some encrypted response using his or her

user name and password information. The gateway then attempts to verify this information first against a local user database (if RADIUS-PAP is enabled) and then by relaying the information to a central authentication server such as a RADIUS server.

➢ **To configure primary and backup RADIUS servers:**

1. Select **VPN > IPSec VPN > RADIUS Client**. The RADIUS Client screen displays:

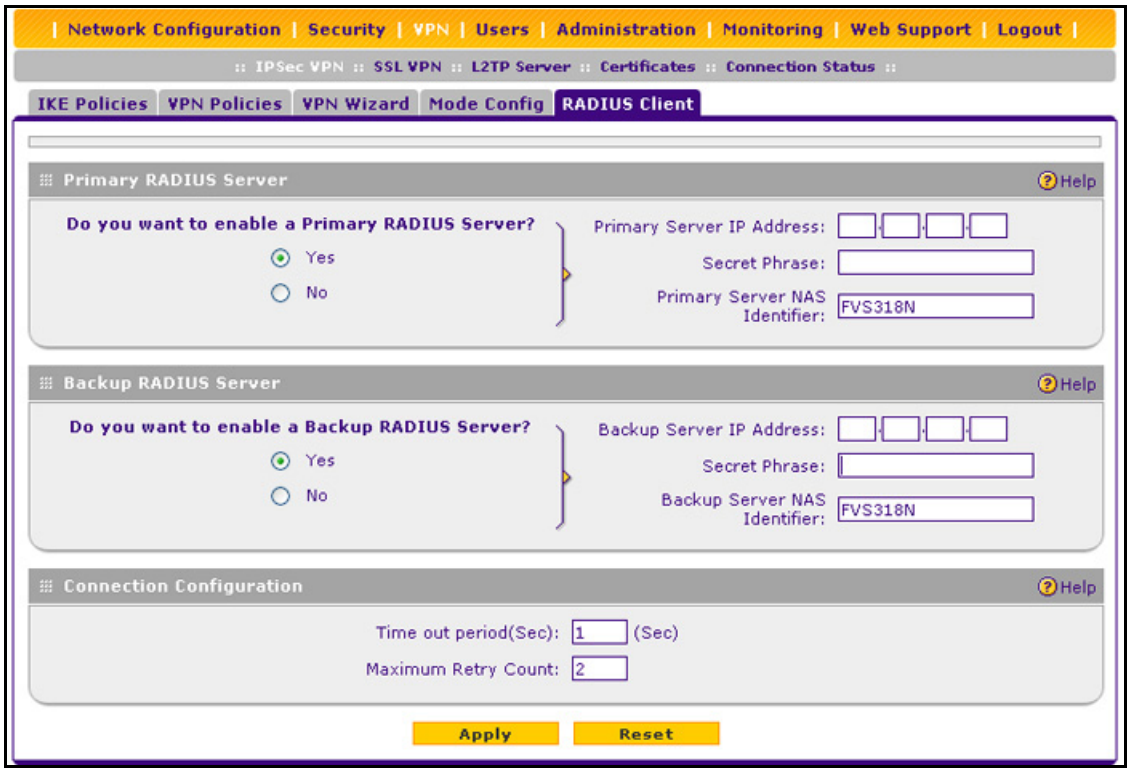


Figure 114.

2. Complete the settings as explained in the following table:

Table 48. RADIUS Client screen settings

Setting	Description
Primary RADIUS Server	
To enable and configure the primary RADIUS server, select the **Yes** radio button, and then enter the settings for the three fields to the right. The default setting is that the No radio button is selected.	
Primary Server IP Address	The IP address of the primary RADIUS server.
Secret Phrase	A shared secret phrase to authenticate the transactions between the client and the primary RADIUS server. The same secret phrase needs to be configured on both the client and the server.

Table 48. RADIUS Client screen settings (continued)

Setting	Description
Primary Server NAS Identifier	The primary Network Access Server (NAS) identifier that needs to be present in a RADIUS request. **Note:** The wireless VPN firewall functions as an NAS, allowing network access to external users after verification of their authentication information. In a RADIUS transaction, the NAS needs to provide some NAS identifier information to the RADIUS server. Depending on the configuration of the RADIUS server, the wireless VPN firewall's IP address might be sufficient as an identifier, or the server might require a name, which you need to enter in this field.
Backup RADIUS Server	
To enable and configure the backup RADIUS server, select the **Yes** radio button, and then enter the settings for the three fields to the right. The default setting is that the No radio button is selected.	
Backup Server IP Address	The IP address of the backup RADIUS server.
Secret Phrase	A shared secret phrase to authenticate the transactions between the client and the backup RADIUS server. The same secret phrase needs to be configured on both the client and the server.
Backup Server NAS Identifier	The backup Network Access Server (NAS) identifier that needs to be present in a RADIUS request. **Note:** See the note earlier in this table for the Primary Server NAS Identifier.
Connection Configuration	
Time out period	The period in seconds that the wireless VPN firewall waits for a response from a RADIUS server. The default setting is 30 seconds.
Maximum Retry Counts	The maximum number of times that the wireless VPN firewall attempts to connect to a RADIUS server. The default setting is 4 retry counts.

3. Click **Apply** to save your settings.

Note: You can select the RADIUS authentication protocol (PAP or CHAP) on the Edit IKE Policy screen or Add IKE Policy screen (see *Configure XAUTH for VPN Clients* on page 195).

Assign IP Addresses to Remote Users (Mode Config)

To simplify the process of connecting remote VPN clients to the wireless VPN firewall, use the Mode Config feature to automatically assign IP addresses to remote users, including a network access IP address, subnet mask, WINS server, and DNS address. Remote users are given IP addresses available in a secured network space so that remote users appear as seamless extensions of the network.

Mode Config Operation

After the IKE Phase 1 negotiation is complete, the VPN connection initiator (which is the remote user with a VPN client) requests the IP configuration settings such as the IP address, subnet mask, WINS server, and DNS address from the wireless VPN firewall. The Mode Config feature allocates an IP address from the configured IP address pool and activates a temporary IPSec policy, using the information that is specified in the Traffic Tunnel Security Level section of the Mode Config record (on the Add Mode Config Record screen that is shown in *Figure 116* on page 200).

Note: After configuring a Mode Config record, you need to manually configure an IKE policy and select the newly created Mode Config record from the Select Mode Config Record drop-down list (see *Configure Mode Config Operation on the Wireless VPN Firewall* on page 199). You do not need to make changes to any VPN policy.

Note: An IP address that is allocated to a VPN client is released only after the VPN client has gracefully disconnected or after the SA liftetime for the connection has timed out.

Configure Mode Config Operation on the Wireless VPN Firewall

To configure Mode Config on the wireless VPN firewall, first create a Mode Config record, and then select the Mode Config record for an IKE policy.

➢ **To configure Mode Config on the wireless VPN firewall:**

1. Select **VPN > IPSec VPN > Mode Config**. The Mode Config screen displays.

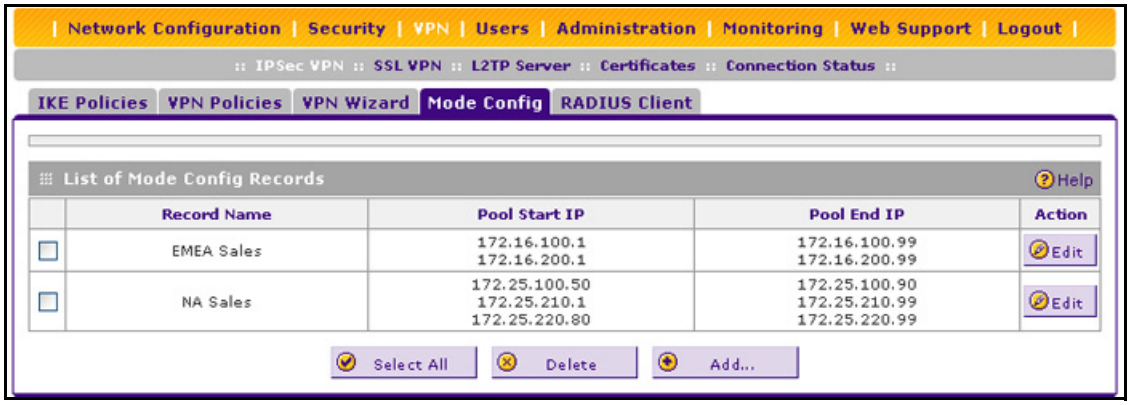


Figure 115.

As an example, the screen shows two Mode Config records with the names EMEA Sales and NA Sales:

- For EMEA Sales, a first pool (172.16.100.1 through 172.16.100.99) and second pool (172.16.200.1 through 172.16.200.99) are shown.
- For NA Sales, a first pool (172.25.100.50 through 172.25.100.99), a second pool (172.25.210.1 through 172.25.210.99), and a third pool (172.25.220.80 through 172.25.220.99) are shown.

2. Under the List of Mode Config Records table, click the **Add** table button. The Add Mode Config Record screen displays:

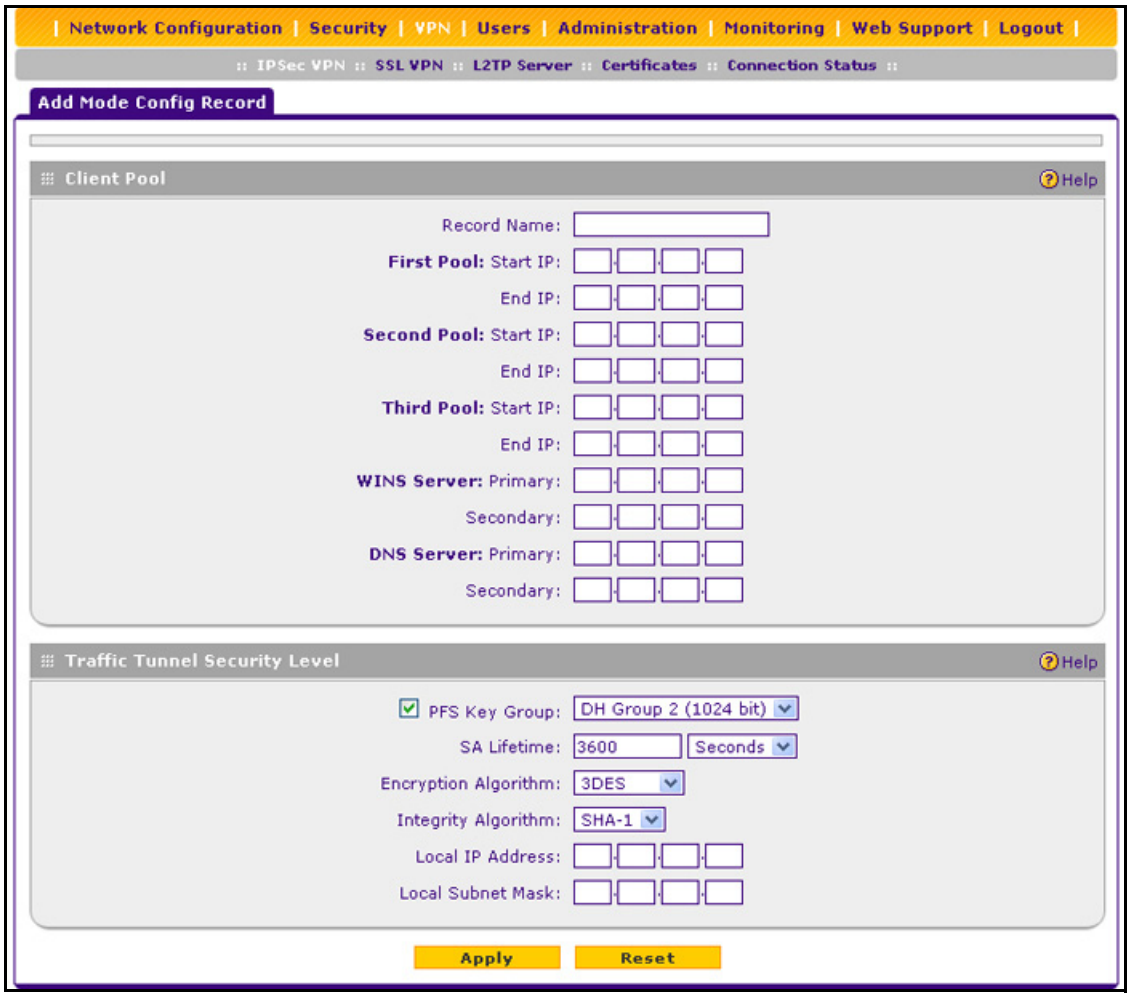


Figure 116.

3. Complete the settings as explained in the following table:

Table 49. Add Mode Config Record screen settings

Setting	Description
Client Pool	
Record Name	A descriptive name of the Mode Config record for identification and management purposes.
First Pool	Assign at least one range of IP pool addresses in the First Pool fields to enable the wireless VPN firewall to allocate these to remote VPN clients. The Second Pool and Third Pool fields are optional. To specify any client pool, enter the starting IP address for the pool in the Starting IP field, and enter the ending IP address for the pool in the Ending IP field. **Note:** No IP pool should be within the range of the local network IP addresses. Use a different range of private IP addresses such as 172.16.xxx.xx.
Second Pool	
Third Pool	
WINS Server	If there is a WINS server on the local network, enter its IP address in the Primary field. You can enter the IP address of a second WINS server in the Secondary field.
DNS Server	Enter the IP address of the DNS server that is used by remote VPN clients in the Primary field. You can enter the IP address of a second DNS server in the Secondary field.
Traffic Tunnel Security Level **Note:** Generally, the default settings work well for a Mode Config configuration.	
PFS Key Group	Select this check box to enable Perfect Forward Secrecy (PFS), and then select a Diffie-Hellman (DH) group from the drop-down list. The DH Group sets the strength of the algorithm in bits. The higher the group, the more secure the exchange. From the drop-down list, select one of the following three strengths: • **Group 1 (768 bit)** • **Group 2 (1024 bit)**. This is the default setting. • **Group 5 (1536 bit)**
SA Lifetime	The lifetime of the security association (SA) is the period or the amount of transmitted data after which the SA becomes invalid and needs to be renegotiated. From the drop-down list, select how the SA lifetime is specified: • **Seconds**. In the SA Lifetime field, enter a period in seconds. The minimum value is 300 seconds. The default setting is 3600 seconds. • **KBytes**. In the SA Lifetime field, enter a number of kilobytes. The minimum value is 1920000 KB.
Encryption Algorithm	From the drop-down list, select one of the following five algorithms to negotiate the security association (SA): • **None**. No encryption. • **DES**. Data Encryption Standard (DES). • **3DES**. Triple DES. This is the default algorithm. • **AES-128**. Advanced Encryption Standard (AES) with a 128-bit key size. • **AES-192**. AES with a 192-bit key size. • **AES-256**. AES with a 256-bit key size.

Table 49. Add Mode Config Record screen settings (continued)

Setting	Description
Integrity Algorithm	From the drop-down list, select one of the following two algorithms to be used in the VPN header for the authentication process: • **SHA-1**. Hash algorithm that produces a 160-bit digest. This is the default setting. • **MD5**. Hash algorithm that produces a 128-bit digest.
Local IP Address	The local IP address to which remote VPN clients have access. If you do not specify a local IP address, the wireless VPN firewall's default LAN IP address is used (by default, 192.168.1.1).
Local Subnet Mask	The local subnet mask. Typically, this is 255.255.255.0. **Note:** If you do not specify a local IP address, you do not need to specify a subnet either.

4. Click **Apply** to save your settings. The new Mode Config record is added to the List of Mode Config Records table.

   Continue the Mode Config configuration procedure by configuring an IKE policy.

5. Select **VPN > IPSec VPN**. The IPSec VPN submenu tabs display with the IKE Policies screen in view (see *Figure 110* on page 180).
6. Under the List of IKE Policies table, click the **Add** table button. The Add IKE Policy screen displays.

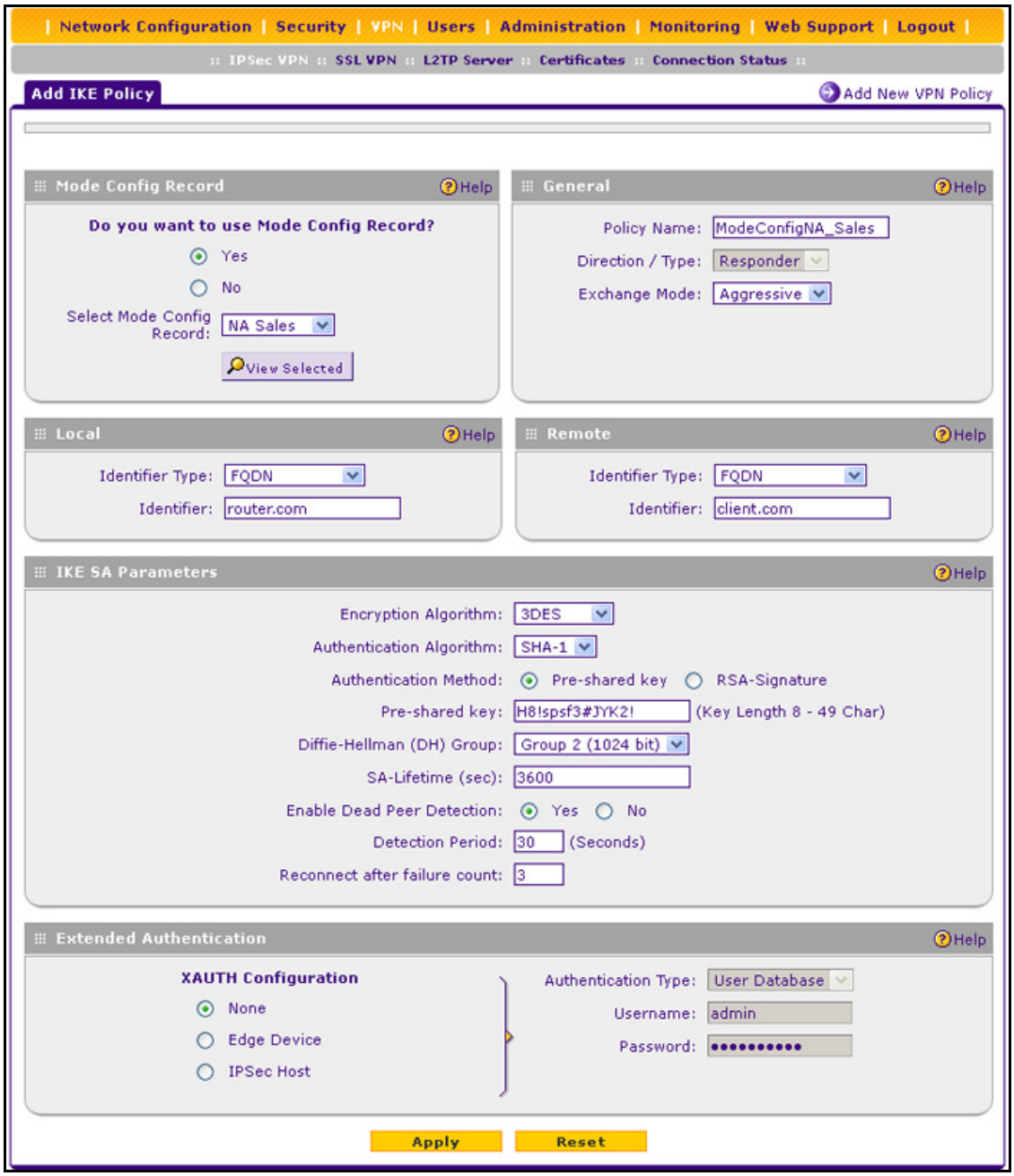


Figure 117.

7. On the Add IKE Policy screen, complete the settings as explained in the following table.

Note: The IKE policy settings that are explained in the following table are specifically for a Mode Config configuration. *Table 44* on page 183 explains the general IKE policy settings.

Table 50. Add IKE Policy screen settings for a Mode Config configuration

Setting	Description	
Mode Config Record		
Do you want to use Mode Config Record?	Select the **Yes** radio button. **Note:** Because Mode Config functions only in Aggressive mode, selecting the Yes radio button sets the tunnel exchange mode to Aggressive mode. Mode Config also requires that both the local and remote endpoints are defined by their FQDNs.	
	Select Mode Config Record	From the drop-down list, select the Mode Config record that you created in *step 4* on page 202. This example uses NA Sales.
General		
Policy Name	A descriptive name of the IKE policy for identification and management purposes. This example uses ModeConfigNA_Sales. **Note:** The name is not supplied to the remote VPN endpoint.	
Direction / Type	Responder is automatically selected when you select the Mode Config record in the Mode Config Record section of the screen. This ensures that the wireless VPN firewall responds to an IKE request from the remote endpoint but does not initiate one.	
Exchange Mode	Aggressive mode is automatically selected when you select the Mode Config record in the Mode Config Record section of the screen.	
Local		
Identifier Type	From the drop-down list, select **FQDN**. **Note:** Mode Config requires that the wireless VPN firewall (that is, the local endpoint) is defined by an FQDN.	
	Identifier	Enter an FQDN for the wireless VPN firewall. This example uses router.com.
Remote		
Identifier Type	From the drop-down list, select **FQDN**. **Note:** Mode Config requires that the remote endpoint is defined by an FQDN.	
	Identifier	Enter the FQDN for the remote endpoint. This needs to be an FQDN that is not used in any other IKE policy. This example uses client.com.

Table 50. Add IKE Policy screen settings for a Mode Config configuration (continued)

Setting	Description	
IKE SA Parameters **Note:** Generally, the default settings work well for a Mode Config configuration.		
Encryption Algorithm	To negotiate the security association (SA), from the drop-down list, select the **3DES** algorithm.	
Authentication Algorithm	From the drop-down list, select the **SHA-1** algorithm to be used in the VPN header for the authentication process.	
Authentication Method	Select **Pre-shared key** as the authentication method, and enter a key in the Pre-shared key field.	
	Pre-shared key	A key with a minimum length of 8 characters and no more than 49 characters. Do not use a double quote (“) in the key. This example uses H8!spsf3#JYK2!.
Diffie-Hellman (DH) Group	The DH Group sets the strength of the algorithm in bits. From the drop-down list, select **Group 2 (1024 bit)**.	
SA-Lifetime (sec)	The period in seconds for which the IKE SA is valid. When the period times out, the next rekeying occurs. The default setting is 28800 seconds (8 hours). However, for a Mode Config configuration, NETGEAR recommends 3600 seconds (1 hour).	
Enable Dead Peer Detection **Note:** See also *Configure Keep-Alives and Dead Peer Detection* on page 215.	Select a radio button to specify whether or not Dead Peer Detection (DPD) is enabled: • **Yes**. This feature is enabled. When the wireless VPN firewall detects an IKE connection failure, it deletes the IPSec and IKE SA and forces a reestablishment of the connection. You need to specify the detection period in the Detection Period field and the maximum number of times that the wireless VPN firewall attempts to reconnect in the Reconnect after failure count field. • **No**. This feature is disabled. This is the default setting.	
	Detection Period	The period in seconds between consecutive DPD R-U-THERE messages, which are sent only when the IPSec traffic is idle. The default setting is 10 seconds. This example uses 30 seconds.
	Reconnect after failure count	The maximum number of DPD failures before the wireless VPN firewall tears down the connection and then attempts to reconnect to the peer. The default setting is 3 failures.

Table 50. Add IKE Policy screen settings for a Mode Config configuration (continued)

Setting	Description	
Extended Authentication		
XAUTH Configuration **Note:** For more information about XAUTH and its authentication modes, see *Configure XAUTH for VPN Clients* on page 195.	Select one of the following radio buttons to specify whether or not Extended Authentication (XAUTH) is enabled, and, if enabled, which device is used to verify user account information: • **None**. XAUTH is disabled. This the default setting. • **Edge Device**. The wireless VPN firewall functions as a VPN concentrator on which one or more gateway tunnels terminate. The authentication modes that are available for this configuration are User Database, RADIUS PAP, and RADIUS CHAP. • **IPSec Host**. The wireless VPN firewall functions as a VPN client of the remote gateway. In this configuration the wireless VPN firewall is authenticated by a remote gateway with a user name and password combination.	
	Authentication Type	For an Edge Device configuration, from the drop-down list, select one of the following authentication types: • **User Database**. XAUTH occurs through the wireless VPN firewall's user database. You can add users on the Add User screen (see *User Database Configuration* on page 196). • **Radius PAP**. XAUTH occurs through RADIUS Password Authentication Protocol (PAP). The local user database is first checked. If the user account is not present in the local user database, the wireless VPN firewall connects to a RADIUS server. For more information, see *RADIUS Client Configuration* on page 196. • **Radius CHAP**. XAUTH occurs through RADIUS Challenge Handshake Authentication Protocol (CHAP). For more information, see *RADIUS Client Configuration* on page 196.
	Username	The user name for XAUTH.
	Password	The password for XAUTH.

8. Click **Apply** to save your settings. The IKE policy is added to the List of IKE Policies table.

Configure the ProSafe VPN Client for Mode Config Operation

When the Mode Config feature is enabled, the following information is negotiated between the VPN client and the wireless VPN firewall during the authentication phase:

- Virtual IP address of the VPN client
- DNS server address (optional)
- WINS server address (optional)

The virtual IP address that is issued by the wireless VPN firewall is displayed in the VPN Client Address field on the VPN client's IPSec pane.

Note: Perform these tasks from a PC that has the NETGEAR ProSafe VPN Client installed.

To configure the VPN client for Mode Config operation, create authentication settings (phase 1 settings), create an associated IPSec configuration (phase 2 settings), and then specify the global parameters.

Configure the Mode Config Authentication Settings (Phase 1 Settings)

➢ **To create new authentication settings:**

1. Right-click the VPN client icon in your Windows system tray, and select **Configuration Panel**. The Configuration Panel screen displays.

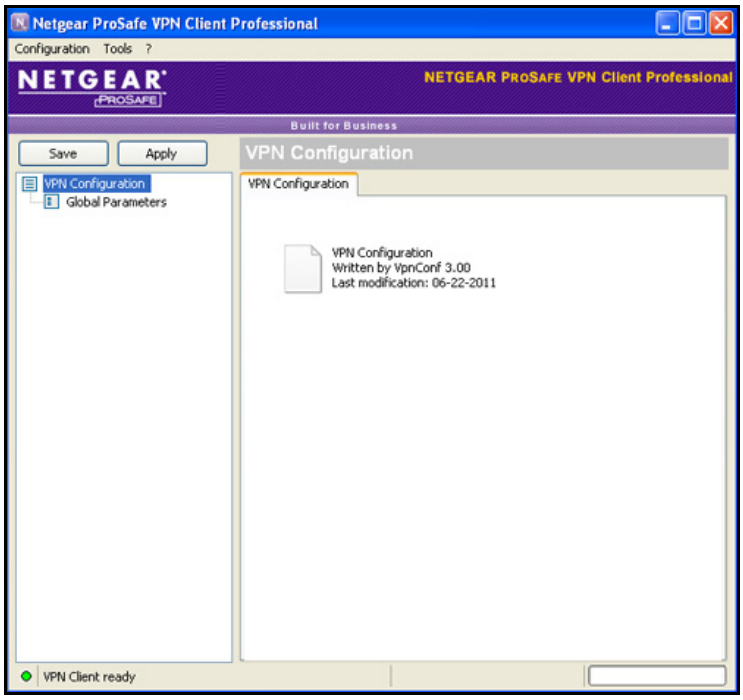


Figure 118.

2. In the tree list pane of the Configuration Panel screen, right-click **VPN Configuration**, and select **New Phase 1**.

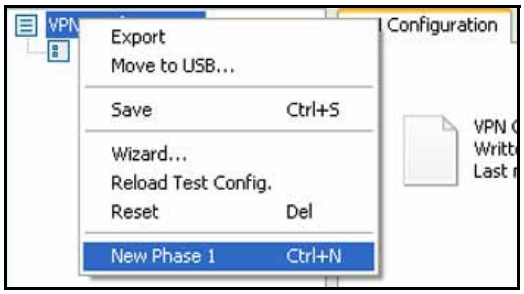


Figure 119.

3. Change the name of the authentication phase (the default is Gateway):
   a. Right-click the authentication phase name.
   b. Select **Rename**.
   c. Type **GW_ModeConfig**.
   d. Click anywhere in the tree list pane.

   Note: *This is the name for the authentication phase that is used only for the VPN client, not during IKE negotiation. You can view and change this name in the tree list pane. This name needs to be a unique name.*

The Authentication pane displays in the Configuration Panel screen, with the Authentication tab selected by default.

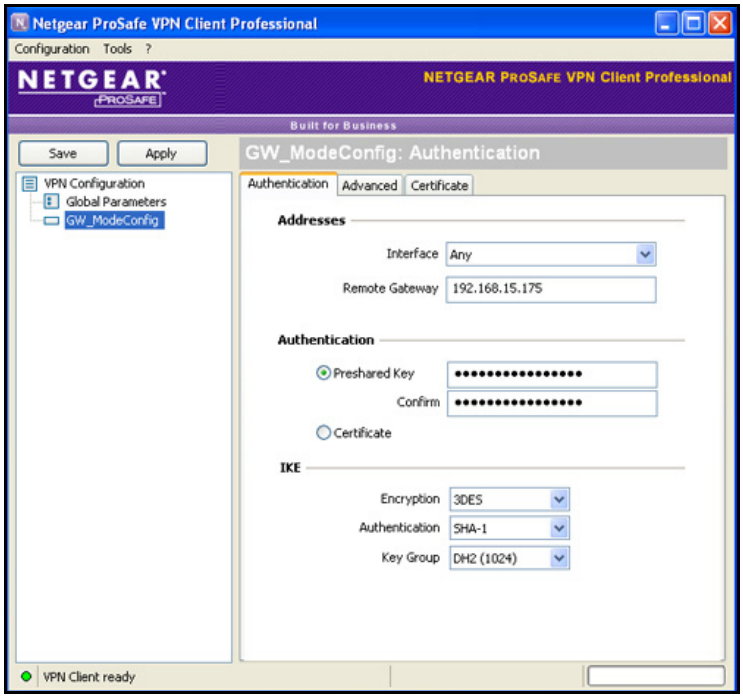


Figure 120.

4. Specify the settings that are explained in the following table.

Table 51. VPN client authentication settings (Mode Config)

Setting	Description	
Interface	Select **Any** from the drop-down list.	
Remote Gateway	Enter the remote IP address or DNS name of the wireless VPN firewall. For example, enter **192.168.15.175**.	
Preshared Key	Select the **Preshared Key** radio button. Enter the pre-shared key that you already specified on the wireless VPN firewall. For example, enter **H8!spsf3#JYK2!**. Confirm the key in the Confirm field.	
IKE	Encryption	Select the **3DES** encryption algorithm from the drop-down list.
	Authentication	Select the **SHA1** authentication algorithm from the drop-down list.
	Key Group	Select the **DH2 (1024)** key group from the drop-down list. **Note:** On the wireless VPN firewall, this key group is referred to as Diffie-Hellman Group 2 (1024 bit).

5. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.
6. Click the **Advanced** tab in the Authentication pane. The Advanced pane displays.

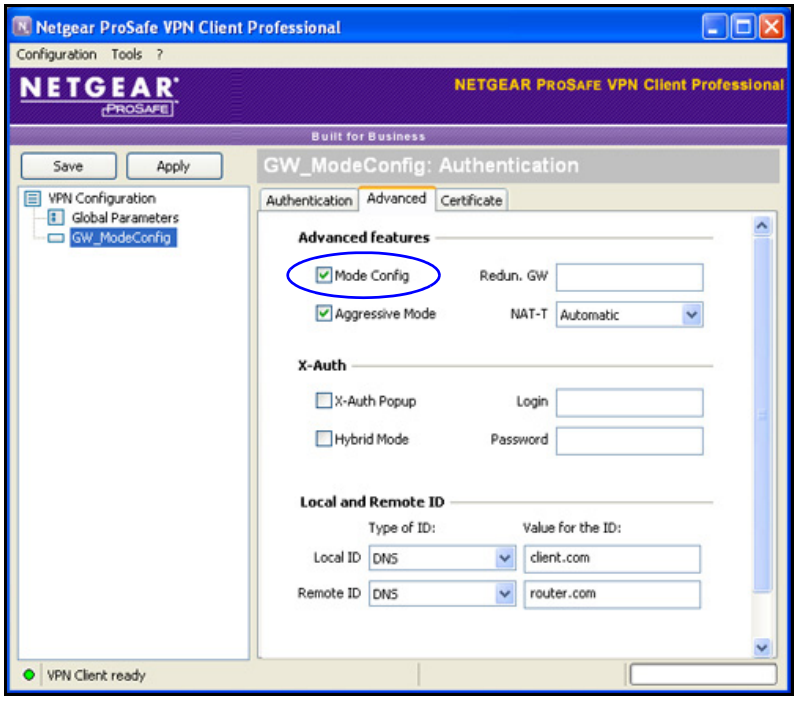


Figure 121.

7. Specify the settings that are explained in the following table.

Table 52. VPN client advanced authentication settings (Mode Config)

Setting	Description
Advanced features	
Mode Config	Select this check box to enable Mode Config.
Aggressive Mode	Select this check box to enable aggressive mode as the mode of negotiation with the wireless VPN firewall.
NAT-T	Select **Automatic** from the drop-down list to enable the VPN client and wireless VPN firewall to negotiate NAT-T.
Local and Remote ID	
Local ID	As the type of ID, select **DNS** from the Local ID drop-down list because you specified FQDN in the wireless VPN firewall configuration. As the value of the ID, enter **client.com** as the local ID for the VPN client. **Note:** The remote ID on the wireless VPN firewall is the local ID on the VPN client.
Remote ID	As the type of ID, select **DNS** from the Remote ID drop-down list because you specified an FQDN in the wireless VPN firewall configuration. As the value of the ID, enter **router.com** as the remote ID for the wireless VPN firewall. **Note:** The local ID on the wireless VPN firewall is the remote ID on the VPN client.

8. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.

Create the Mode Config IPSec Configuration (Phase 2 Settings)

Note: On the wireless VPN firewall, the IPSec configuration (phase 2 settings) is referred to as the IKE settings.

➢ **To create an IPSec configuration:**

1. In the tree list pane of the Configuration Panel screen, right-click the **GW_ModeConfig** authentication phase name, and then select **New Phase 2**.
2. Change the name of the IPSec configuration (the default is Tunnel):
   a. Right-click the IPSec configuration name.
   b. Select **Rename**.
   c. Type **Tunnel_ModeConfig**.
   d. Click anywhere in the tree list pane.

Note: *This is the name for the IPSec configuration that is used only for the VPN client, not during IPSec negotiation. You can view and change this name in the tree list pane. This name needs to be a unique name.*

The IPSec pane displays in the Configuration Panel screen, with the IPSec tab selected by default.

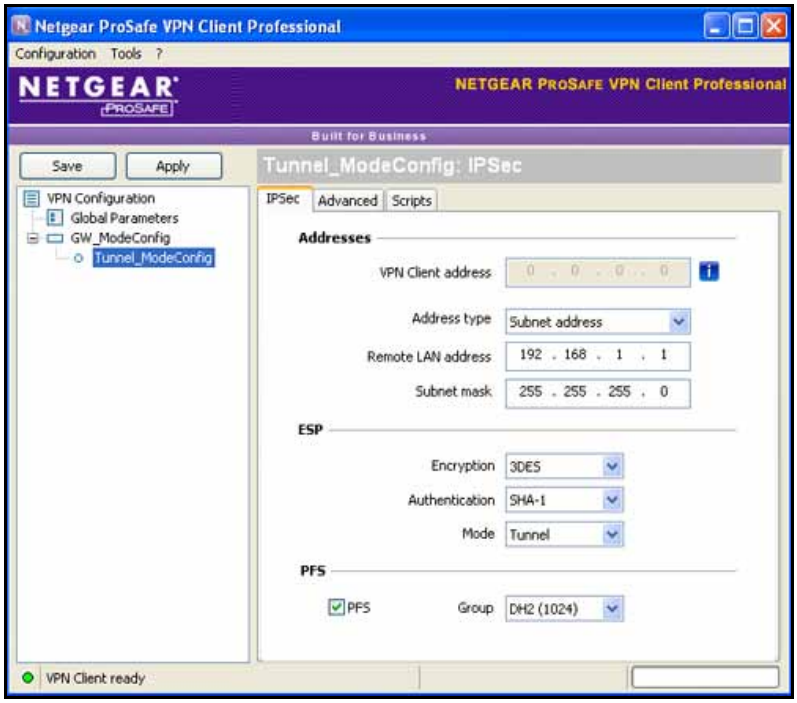


Figure 122.

3. Specify the settings that are explained in the following table.

Table 53. VPN client IPSec configuration settings (Mode Config)

Setting	Description
VPN Client address	This field is masked out because Mode Config is selected. After an IPSec connection is established, the IP address that is issued by the wireless VPN firewall displays in this field (see *Figure 127* on page 215).
Address Type	Select **Subnet address** from the drop-down list.
Remote host address	The address that you need to enter depends on whether or not you have specified a LAN IP network address in the Local IP Address field on the Add Mode Config Record screen of the wireless VPN firewall: • If you left the Local IP Address field blank, enter the wireless VPN firewall's default LAN IP address as the remote host address that opens the VPN tunnel. For example, enter **192.168.1.1**. • If you specified a LAN IP network address in the Local IP Address field, enter the address that you specified as the remote host address that opens the VPN tunnel.

Table 53. VPN client IPSec configuration settings (Mode Config) (continued)

Setting	Description	
Subnet mask	Enter **255.255.255.0** as the remote subnet mask of the wireless VPN firewall that opens the VPN tunnel. This is the LAN IP subnet mask that you specified in the Local Subnet Mask field on the Add Mode Config Record screen of the wireless VPN firewall. If you left the Local Subnet Mask field blank, enter the wireless VPN firewall's default IP subnet mask.	
ESP	Encryption	Select **3DES** as the encryption algorithm from the drop-down list.
	Authentication	Select **SHA-1** as the authentication algorithm from the drop-down list.
	Mode	Select **Tunnel** as the encapsulation mode from the drop-down list.
PFS and Group	Select the **PFS** check box, and then select the **DH2 (1024)** key group from the drop-down list. **Note:** On the wireless VPN firewall, this key group is referred to as Diffie-Hellman Group 2 (1024 bit).	

4. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.

Configure the Mode Config Global Parameters

➢ **To specify the global parameters:**

1. Click **Global Parameters** in the left column of the Configuration Panel screen. The Global Parameters pane displays in the Configuration Panel screen.

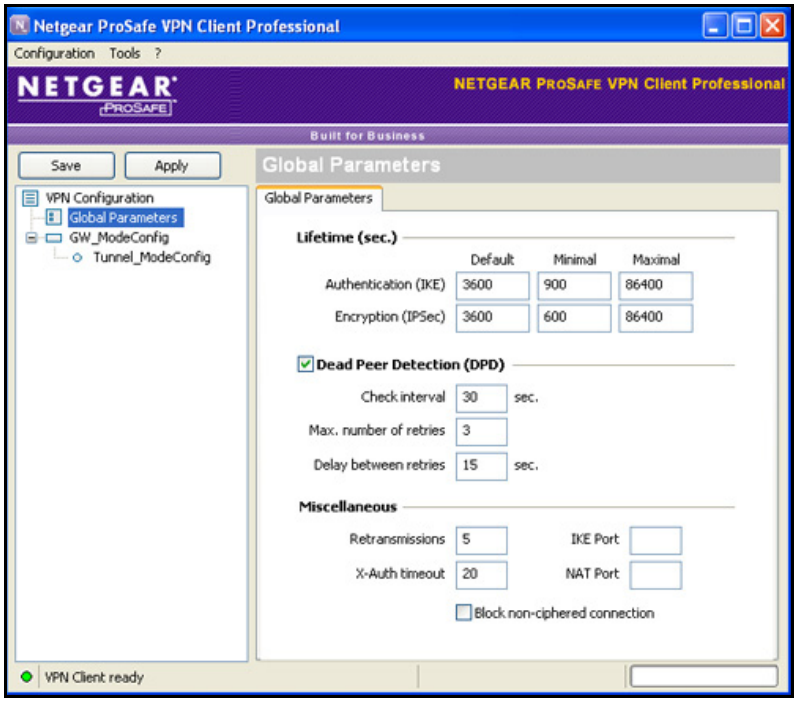


Figure 123.

2. Specify the following default lifetimes in seconds to match the configuration on the wireless VPN firewall:
   - **Authentication (IKE)**, **Default**. Enter **3600** seconds.
   - **Encryption (IPSec)**, **Default**. Enter **3600** seconds.
3. Select the **Dead Peer Detection (DPD)** check box, and configure the following DPD settings to match the configuration on the wireless VPN firewall:
   - **Check Interval**. Enter **30** seconds.
   - **Max. number of entries**. Enter **3** retries.
   - **Delay between entries**. Leave the default delay setting of 15 seconds.
4. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.

The Mode Config configuration of the VPN client is now complete.

Test the Mode Config Connection

➢ **To test the Mode Config connection from the VPN client to the wireless VPN firewall:**

1. Right-click the system tray icon, and select **Open tunnel 'Tunnel_ModeConfig'**.

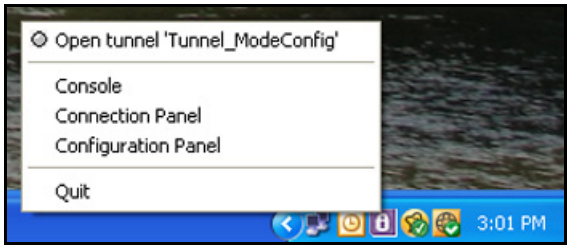


Figure 124.

When the tunnel opens successfully, the *Tunnel opened* message displays above the system tray, and the VPN client displays a green icon in the system tray.

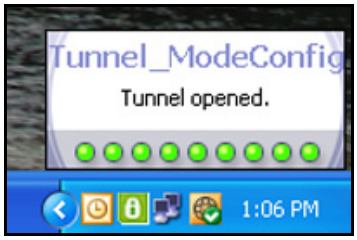


Figure 125.

2. Verify that the wireless VPN firewall issued an IP address to the VPN client. This IP address displays in the VPN Client address field on the IPSec pane of the VPN client. (The following figure shows the upper part of the IPSec pane only.)

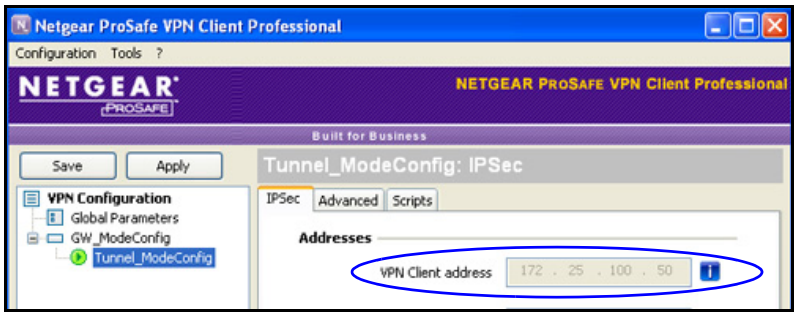


Figure 126.

3. From the client PC, ping a computer on the wireless VPN firewall LAN.

Modify or Delete a Mode Config Record

Note: Before you modify or delete a Mode Config record, make sure it is not used in an IKE policy.

➢ **To edit a Mode Config record:**

1. On the Mode Config screen (see *Figure 115* on page 199), click the **Edit** button in the Action column for the record that you want to modify. The Edit Mode Config Record screen displays. This screen is identical to the Add Mode Config Record screen (see *Figure 116* on page 200).
2. Modify the settings as explained in *Table 49* on page 201.
3. Click **Apply** to save your settings.

➢ **To delete one or more Mode Config records:**

1. On the Mode Config screen (see *Figure 115* on page 199), select the check box to the left of each record that you want to delete, or click the **Select All** table button to select all records.
2. Click the **Delete** table button.

Configure Keep-Alives and Dead Peer Detection

In some cases, you might not want a VPN tunnel to be disconnected when traffic is idle, for example, when client-server applications over the tunnel cannot tolerate the tunnel establishment time. If you require a VPN tunnel to remain connected, you can use the keep-alive and Dead Peer Detection (DPD) features to prevent the tunnel from being disconnected and to force a reconnection if the tunnel disconnects for any reason.

For DPD to function, the peer VPN device on the other end of the tunnel also needs to support DPD. Keep-alive, though less reliable than DPD, does not require any support from the peer device.

Configure Keep-Alives

The keep-alive feature maintains the IPSec SA by sending periodic ping requests to a host across the tunnel and monitoring the replies.

➤ **To configure the keep-alive feature on a configured VPN policy:**

1. Select **VPN > IPSec VPN > VPN Policies**. The VPN Policies screen displays (see *Figure 112* on page 188).
2. In the List of VPN Policies table, click the **Edit** table button to the right of the VPN policy that you want to edit. The Edit VPN Policy screen displays. (The following figure shows only the top part with the General section.)

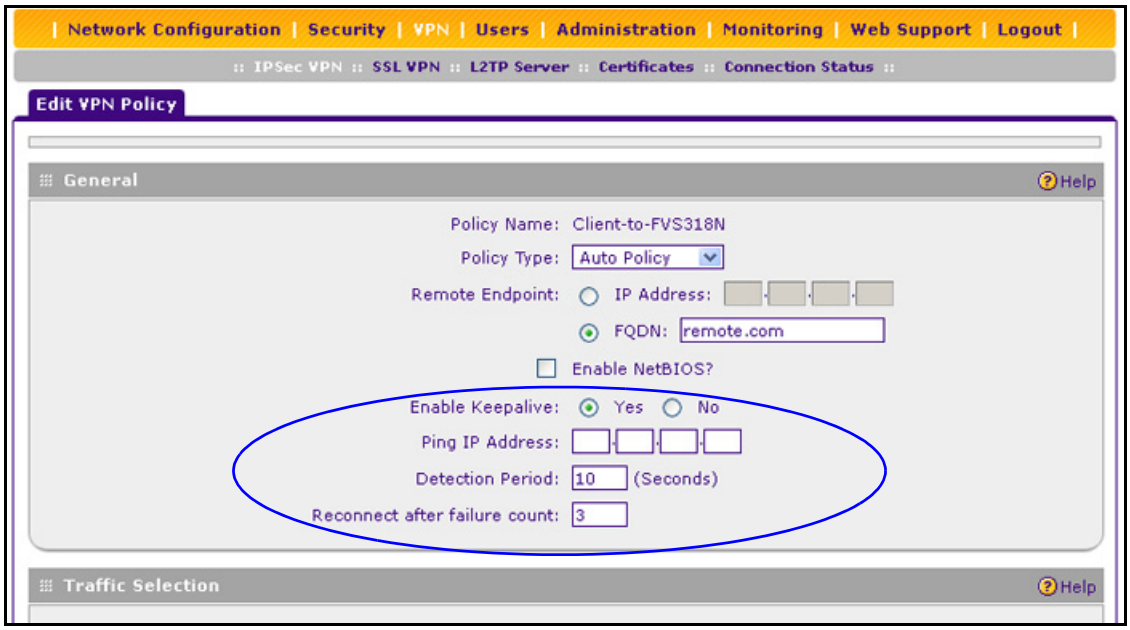

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
IPSec VPN :: SSL VPN :: L2TP Server :: Certificates :: Connection Status ::
Edit VPN Policy
General
Help
Policy Name: Client-to-FVS318N
Policy Type: Auto Policy
Remote Endpoint: IP Address:
FQDN: remote.com
Enable NetBIOS?
Enable Keepalive: Yes No
Ping IP Address:
Detection Period: 10 (Seconds)
Reconnect after failure count: 3
Traffic Selection
Help

Figure 127.

3. Enter the settings as explained in the following table:

Table 54. Keep-alive settings

Setting	Description	
General		
Enable Keepalive	Select the **Yes** radio button to enable the keep-alive feature. Periodically, the wireless VPN firewall sends keep-alive requests (ping packets) to the remote endpoint to keep the tunnel alive. You need to specify the ping IP address in the Ping IP Address field, the detection period in the Detection Period field, and the maximum number of keep-alive requests that the wireless VPN firewall sends in the Reconnect after failure count field.	
	Ping IP Address	The IP address that the wireless VPN firewall pings. The address should be of a host that can respond to ICMP ping requests.
	Detection Period	The period in seconds between the keep-alive requests. The default setting is 10 seconds.
	Reconnect after failure count	The maximum number of keep-alive requests before the wireless VPN firewall tears down the connection and then attempts to reconnect to the remote endpoint. The default setting is 3 keep-alive requests.

4. Click **Apply** to save your settings.

Configure Dead Peer Detection

The Dead Peer Detection (DPD) feature lets the wireless VPN firewall maintain the IKE SA by exchanging periodic messages with the remote VPN peer.

➢ **To configure DPD on a configured IKE policy:**

1. Select **VPN > IPSec VPN**. The IPSec VPN submenu tabs display with the IKE Policies screen in view (see *Figure 110* on page 180).
2. In the List of IKE Policies table, click the **Edit** table button to the right of the IKE policy that you want to edit. The Edit IKE Policy screen displays. (The following figure shows only the IKE SA Parameters section of the screen).

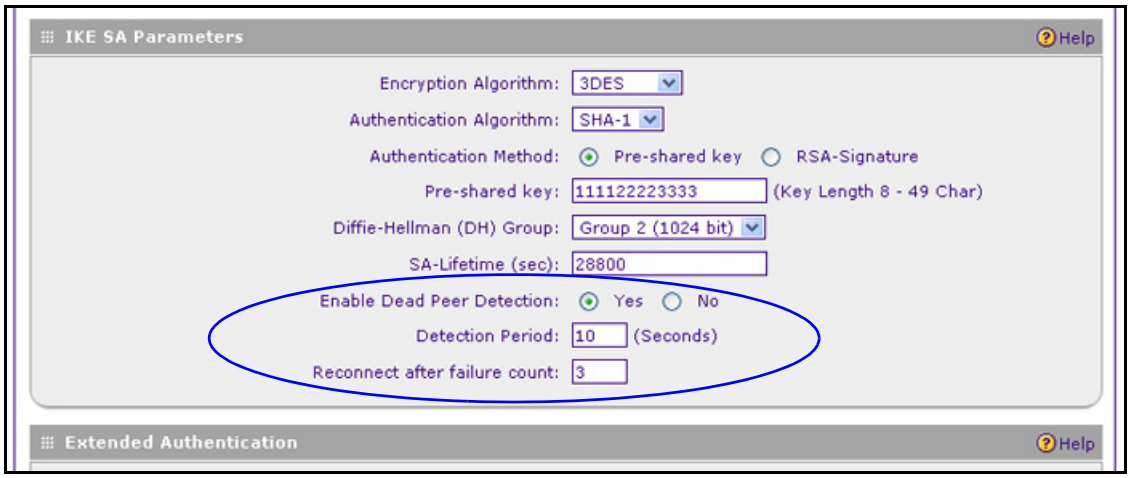

IKE SA Parameters
Help
Encryption Algorithm: 3DES
Authentication Algorithm: SHA-1
Authentication Method: Pre-shared key RSA-Signature
Pre-shared key: 111122223333 (Key Length 8 - 49 Char)
Diffie-Hellman (DH) Group: Group 2 (1024 bit)
SA-Lifetime (sec): 28800
Enable Dead Peer Detection: Yes No
Detection Period: 10 (Seconds)
Reconnect after failure count: 3
Extended Authentication
Help

Figure 128.

3. In the IKE SA Parameters section of the screen, locate the DPD fields, and complete the settings as explained the following table:

Table 55. Dead Peer Detection settings

Setting	Description	
IKE SA Parameters		
Enable Dead Peer Detection	Select the **Yes** radio button to enable DPD. When the wireless VPN firewall detects an IKE connection failure, it deletes the IPSec and IKE SA and forces a reestablishment of the connection. You need to specify the detection period in the Detection Period field and the maximum number of times that the wireless VPN firewall attempts to reconnect in the Reconnect after failure count field.	
	Detection Period	The period in seconds between consecutive DPD R-U-THERE messages, which are sent only when the IPSec traffic is idle. The default setting is 10 seconds.
	Reconnect after failure count	The maximum number of DPD failures before the wireless VPN firewall tears down the connection and then attempts to reconnect to the peer. The default setting is 3 failures.

4. Click **Apply** to save your settings.

Configure NetBIOS Bridging with IPSec VPN

Windows networks use the Network Basic Input/Output System (NetBIOS) for several basic network services such as naming and neighborhood device discovery. Because VPN routers do not usually pass NetBIOS traffic, these network services do not function for hosts on opposite ends of a VPN connection. To solve this problem, you can configure the wireless VPN firewall to bridge NetBIOS traffic over the VPN tunnel.

➢ **To enable NetBIOS bridging on a configured VPN tunnel:**

1. Select **VPN > IPSec VPN > VPN Policies**. The VPN Policies screen displays (see *Figure 112* on page 188).
2. In the List of VPN Policies table, click the **Edit** table button to the right of the VPN policy that you want to edit. The Edit VPN Policy screen displays. (The following figure shows only the top part with the General section.)

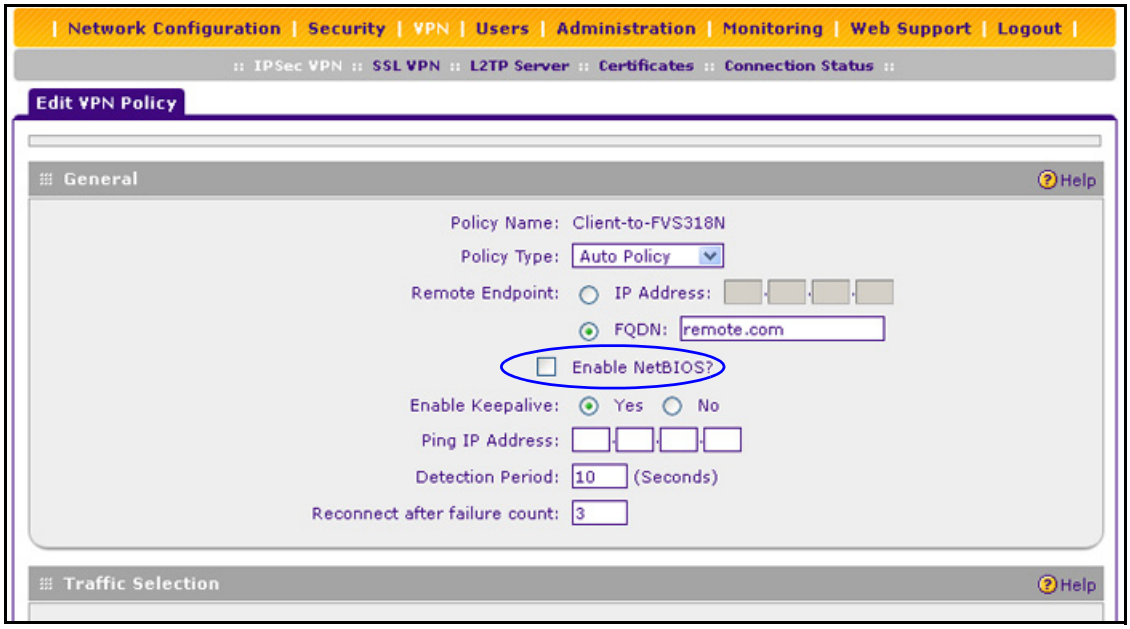

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
IPSec VPN :: SSL VPN :: L2TP Server :: Certificates :: Connection Status
Edit VPN Policy
General
Help
Policy Name: Client-to-FVS318N
Policy Type: Auto Policy
Remote Endpoint: IP Address:
FQDN: remote.com
Enable NetBIOS?
Enable Keepalive: Yes No
Ping IP Address:
Detection Period: 10 (Seconds)
Reconnect after failure count: 3
Traffic Selection
Help

Figure 129.

3. Select the **Enable NetBIOS** check box.
4. Click **Apply** to save your settings.

Configure the L2TP Server

As an alternate solution to IPSec VPN tunnels, you can configure a Layer 2 Tunneling Protocol (L2TP) server on the wireless VPN firewall to allow users to access L2TP clients over L2TP tunnels.

An L2TP Access Concentrator (LAC) typically initiates a tunnel to fullfil a connection request from an L2TP user; the L2TP server accommodates the tunnel request. After an L2TP tunnel is established, the L2TP user can connect to an L2TP client that is located behind the wireless VPN firewall.

Note: IPSec VPN provides stronger authentication and encryption than L2TP. (Packets that traverse the L2TP tunnel are not encapsulated by IPSec.)

You need to enable the L2TP server on the wireless VPN firewall, specify an L2TP server address pool, and create L2TP user accounts. For information about how to create L2TP user accounts, see *Configure User Accounts* on page 254.

➢ **To enable the L2TP server and configure the L2TP server pool:**

1. Select **VPN > L2TP Server**. The L2TP Server screen displays.

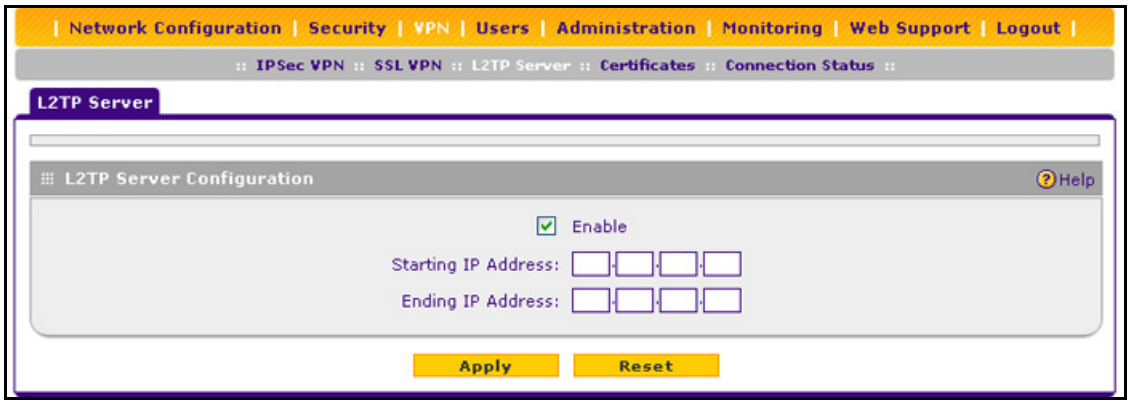

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
IPSec VPN :: SSL VPN :: L2TP Server :: Certificates :: Connection Status
L2TP Server
L2TP Server Configuration
Help
Enable
Starting IP Address:
Ending IP Address:
Apply
Reset

Figure 130.

2. To enable the L2TP server, select the **Enable** check box.
3. Specify the L2TP server address pool with a maximum of 24 IP addresses:
   - In the Starting IP Address fields, type the first address of the pool.
   - In the Ending IP Address fields, type the last address of the pool.
4. Click **Apply** to save your settings.

View the Active L2TP Users

To view the active L2TP tunnel users, select **VPN > Connection Status > L2TP Active Users**. The L2TP Active Users screen displays:

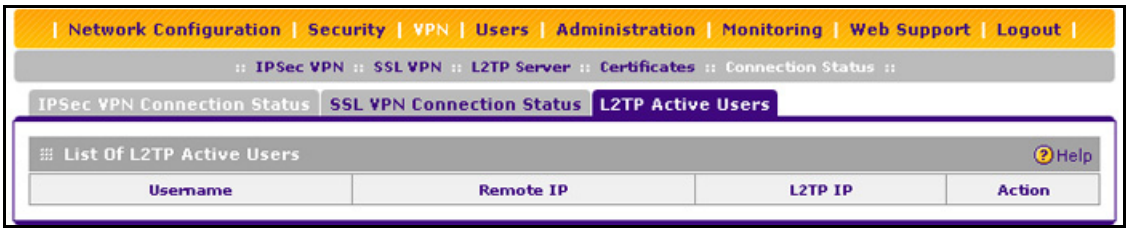

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
IPSec VPN :: SSL VPN :: L2TP Server :: Certificates :: Connection Status
IPSec VPN Connection Status
SSL VPN Connection Status
L2TP Active Users
List Of L2TP Active Users
Help
Username
Remote IP
L2TP IP
Action

Figure 131.

The List of L2TP Active Users table lists each active connection with the information that is described in the following table.

Table 56. L2TP Active Users screen information

Item	Description
Username	The name of the L2TP user that you have defined (see *Configure User Accounts* on page 254).
Remote IP	The client's IP address on the remote LAC.
L2TP IP	The IP address that is assigned by the L2TP server on the wireless VPN firewall.
Action	This column is not applicable to L2TP.

Virtual Private Networking Using IPv4 SSL Connections

7

The wireless VPN firewall provides a hardware-based SSL VPN solution designed specifically to provide remote access for mobile users to their corporate resources, bypassing the need for a preinstalled VPN client on their computers. Using the familiar Secure Sockets Layer (SSL) protocol, commonly used for e-commerce transactions, the wireless VPN firewall can authenticate itself to an SSL-enabled client, such as a standard web browser. Once the authentication and negotiation of encryption information are completed, the server and client can establish an encrypted connection. With support for up to 5 dedicated SSL VPN tunnels, the wireless VPN firewall allows users to easily access the remote network for a customizable, secure, user portal experience from virtually any available platform.

This chapter contains the following sections:

- *SSL VPN Portal Options*
- *Overview of the SSL Configuration Process*
- *Configure Domains, Groups, and Users*
- *Configure Applications for Port Forwarding*
- *Configure the SSL VPN Client*
- *Use Network Resource Objects to Simplify Policies*
- *Configure User, Group, and Global Policies*
- *Access the New SSL Portal Login Screen*

Note: In this release, the wireless VPN firewall supports SSL VPN connections for IPv4 traffic only. By themselves IPv6 addresses provide a much higher level of security than IPv4 addresses, and future releases will support SSL VPN connections for IPv6 traffic.

SSL VPN Portal Options

The wireless VPN firewall's SSL VPN portal can provide two levels of SSL service to the remote user:

- **SSL VPN tunnel**. The wireless VPN firewall can provide the full network connectivity of a VPN tunnel using the remote user's browser instead of a traditional IPSec VPN client. The SSL capability of the user's browser provides authentication and encryption, establishing a secure connection to the wireless VPN firewall. Upon successful connection, an ActiveX-based SSL VPN client is downloaded to the remote PC to allow the remote user to virtually join the corporate network.

  The SSL VPN client provides a point-to-point (PPP) connection between the client and the wireless VPN firewall, and a virtual network interface is created on the user's PC. The wireless VPN firewall assigns the PC an IP address and DNS server IP addresses, allowing the remote PC to access network resources in the same manner as if it were connected directly to the corporate network, subject to any policy restrictions that you configure.

- **SSL port forwarding**. Like an SSL VPN tunnel, port forwarding is a web-based client that is installed transparently and then creates a virtual, encrypted tunnel to the remote network. However, port forwarding differs from an SSL VPN tunnel in several ways:
  - Port forwarding supports only TCP connections, not UDP connections or connections using other IP protocols.
  - Port forwarding detects and reroutes individual data streams on the user's PC to the port-forwarding connection rather than opening up a full tunnel to the corporate network.
  - Port forwarding offers more fine-grained management than an SSL VPN tunnel. You define individual applications and resources that are available to remote users.

The SSL VPN portal can present the remote user with one or both of these SSL service levels, depending on how you set up the configuration.

Overview of the SSL Configuration Process

To configure and activate SSL connections, perform the following six basic steps in the order that they are presented:

1. Create a new SSL portal (see *Create the Portal Layout* on page 223).

   When remote users log in to the wireless VPN firewall, they see a portal page that you can customize to present the resources and functions that you choose to make available.

2. Create authentication domains, user groups, and user accounts (see *Configure Domains, Groups, and Users* on page 227).)
   a. Create one or more authentication domains for authentication of SSL VPN users.

      When remote users log in to the wireless VPN firewall, they need to specify a domain to which their login account belongs. The domain determines the authentication

method that is used and the portal layout that is presented, which in turn determines the network resources to which the users are granted access. Because you need to assign a portal layout when creating a domain, the domain is created after you have created the portal layout.

b. Create one or more groups for your SSL VPN users.

When you define the SSL VPN policies that determine network resource access for your SSL VPN users, you can define global policies, group policies, or individual policies. Because you need to assign an authentication domain when creating a group, the group is created after you have created the domain.

c. Create one or more SSL VPN user accounts.

Because you need to assign a group when creating a SSL VPN user account, the user account is created after you have created the group.

3. For port forwarding, define the servers and services (see *Configure Applications for Port Forwarding* on page 227).

   Create a list of servers and services that can be made available through user, group, or global policies. You can also associate fully qualified domain names (FQDNs) with these servers. The wireless VPN firewall resolves the names to the servers using the list you have created.

4. For SSL VPN tunnel service, configure the virtual network adapter (see *Configure the SSL VPN Client* on page 230).

   For the SSL VPN tunnel option, the wireless VPN firewall creates a virtual network adapter on the remote PC that then functions as if it were on the local network. Configure the portal's SSL VPN client to define a pool of local IP addresses to be issued to remote clients, as well as DNS addresses. Declare static routes or grant full access to the local network, subject to additional policies.

5. To simplify policies, define network resource objects (see *Use Network Resource Objects to Simplify Policies* on page 233).

   Network resource objects are groups of IP addresses, IP address ranges, and services. By defining resource objects, you can more quickly create and configure network policies.

6. Configure the SSL VPN policies (see *Configure User, Group, and Global Policies* on page 235).

   Policies determine access to network resources and addresses for individual users, groups, or everyone.

Create the Portal Layout

The Portal Layouts screen that you can access from the SSL VPN configuration menu allows you to create a custom page that remote users see when they log in to the portal. Because the page is completely customizable, it provides an ideal way to communicate remote access instructions, support information, technical contact information, or VPN-related news updates to remote users. The page is also well suited as a starting page for restricted users; if mobile

users or business partners are permitted to access only a few resources, the page that you create presents only the resources that are relevant to these users.

You apply portal layouts by selecting one from the available portal layouts in the configuration of a domain. When you have completed your portal layout, you can apply the portal layout to one or more authentication domains (see *Configure Domains* on page 247). You can also make the new portal the default portal for the SSL VPN gateway by selecting the default radio button adjacent to the portal layout name.

Note: The Wireless VPN Firewall's default portal address is https://<IP_Address>/portal/SSL-VPN. The default domain geardomain is assigned to the default SSL-VPN portal.

You can define individual layouts for the SSL VPN portal. The layout configuration includes the menu layout, theme, portal pages to display, and web cache control options. The default portal layout is the SSL-VPN portal. You can add additional portal layouts. You can also make any portal the default portal for the wireless VPN firewall by clicking the **Default** button in the Action column of the List of Layouts table, to the right of the desired portal layout.

➢ **To create a new SSL VPN portal layout:**

1. Select **VPN > SSL VPN > Portal Layouts**. The Portal Layouts screen displays. (The following figure shows an additional layout in the List of Layouts table as an example.)

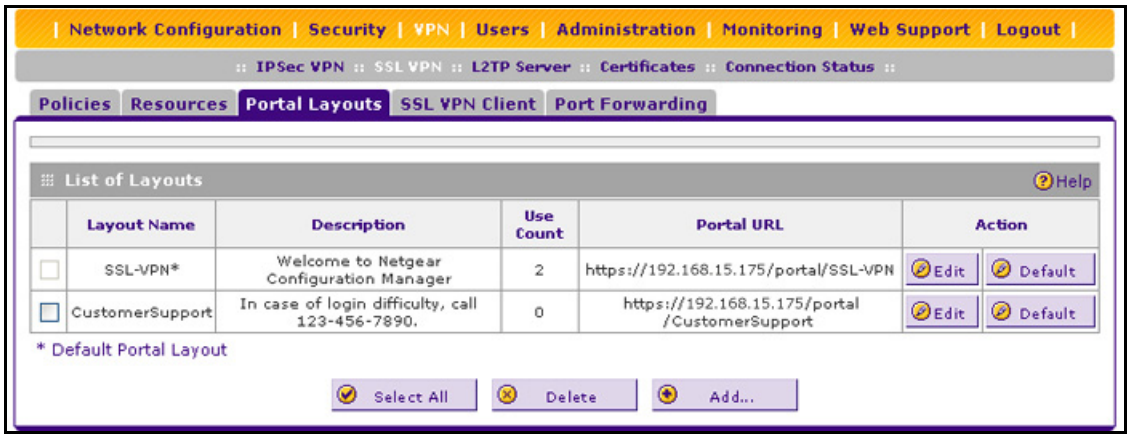


Figure 132.

The List of Layouts table displays the following fields:

- **Layout Name**. The descriptive name of the portal.
- **Description**. The banner message that is displayed at the top of the portal (see *Figure 140* on page 241).
- **Use Count**. The number of remote users that are currently using the portal.

- **Portal URL**. The URL at which the portal can be accessed.
- **Action**. The table buttons, which allow you to edit the portal layout or set it as the default.

2. Under the List of Layouts table, click the **Add** table button. The Add Portal Layout screen displays. (The following figure shows an example.)

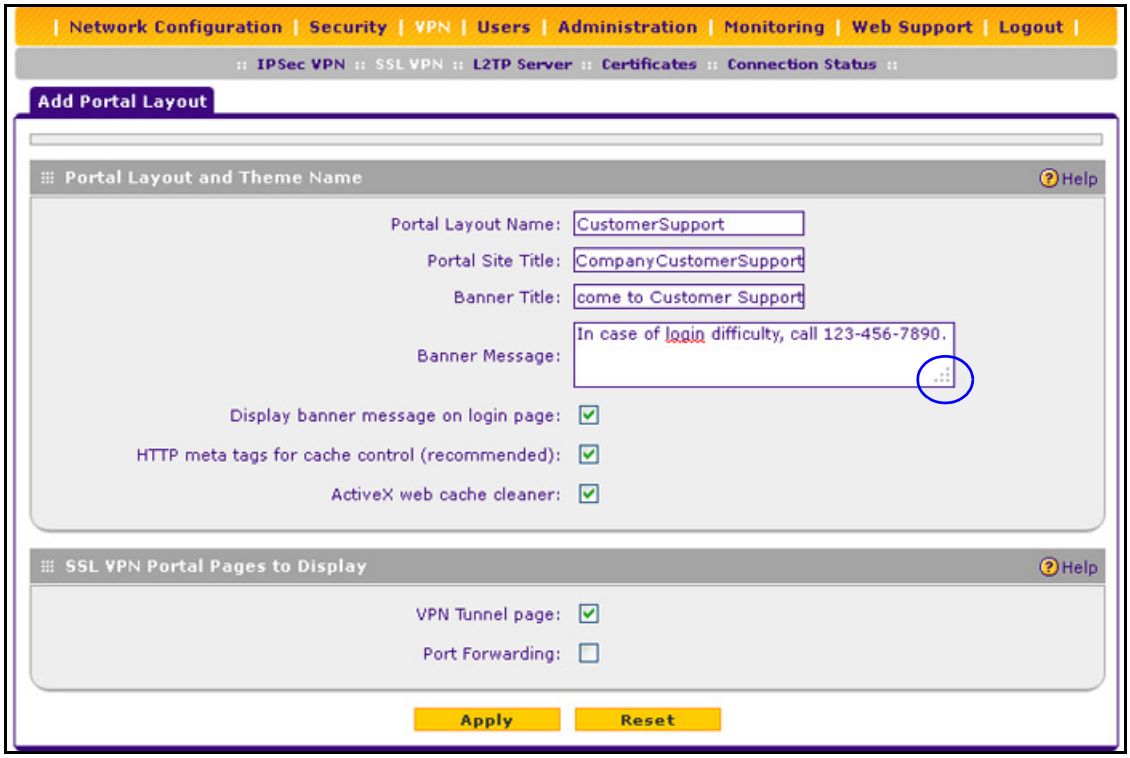

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
IPSec VPN :: SSL VPN :: L2TP Server :: Certificates :: Connection Status
Add Portal Layout
Portal Layout and Theme Name
Help
Portal Layout Name:
CustomerSupport
Portal Site Title:
CompanyCustomerSupport
Banner Title:
come to Customer Support
Banner Message:
In case of login difficulty, call 123-456-7890.
Display banner message on login page:
HTTP meta tags for cache control (recommended):
ActiveX web cache cleaner:
SSL VPN Portal Pages to Display
Help
VPN Tunnel page:
Port Forwarding:
Apply
Reset

Figure 133.

3. Complete the settings as explained in the following table:

Table 57. Add Portal Layout screen settings

Setting	Description
Portal Layout and Theme Name	
Portal Layout Name	A descriptive name for the portal layout. This name is part of the path of the SSL VPN portal URL. **Note:** Custom portals are accessed at a different URL than the default portal. For example, if your SSL VPN portal is hosted at https://vpn.company.com, and you create a portal layout named CustomerSupport, then users access the website at https://vpn.company.com/portal/CustomerSupport. **Note:** Only alphanumeric characters, hyphens (-), and underscores (_) are accepted in the Portal Layout Name field. If you enter other types of characters or spaces, the layout name is truncated before the first nonalphanumeric character. **Note:** Unlike most other URLs, this name is case-sensitive.

Table 57. Add Portal Layout screen settings (continued)

Setting	Description
Portal Site Title	The title that displays at the top of the user's web browser window, for example, *Company Customer Support*.
Banner Title	The banner title of a banner message that users see before they log in to the portal, for example, *Welcome to Customer Support*. **Note:** For an example, see *Figure 140* on page 241. The banner title text is displayed in the orange header bar.
Banner Message	The text of a banner message that users see before they log in to the portal, for example, *In case of login difficulty, call 123-456-7890*. Enter a plain text message, or include HTML and JavaScript tags. The maximum length of the login screen message is 4096 characters. **Note:** You can enlarge the field (that is, the text box) by manipulating the lower right corner of the field. **Note:** For an example, see *Figure 140* on page 241. The banner message text is displayed in the gray header bar.
Display banner message on login page	Select this check box to show the banner title and banner message text on the login screen as shown in *Figure 140* on page 241.
HTTP meta tags for cache control (recommended)	Select this check box to apply cache control directives for the HTTP meta tags to this portal layout. Cache control directives include: <meta http-equiv="pragma" content="no-cache"> <meta http-equiv="cache-control" content="no-cache"> <meta http-equiv="cache-control" content="must-revalidate"> **Note:** NETGEAR strongly recommends enabling HTTP meta tags for security reasons and to prevent out-of-date web pages, themes, and data being stored in a user's web browser cache.
ActiveX web cache cleaner	Select this check box to enable ActiveX cache control to be loaded when users log in to the SSL VPN portal. The web cache cleaner prompts the user to delete all temporary Internet files, cookies, and browser history when the user logs out or closes the web browser window. The ActiveX web cache control is ignored by web browsers that do not support ActiveX.
SSL VPN Portal Pages to Display	
VPN Tunnel page	To provide full network connectivity, select this check box.
Port Forwarding	To specific defined network services, select this check box to provide access. **Note:** Any pages that are not selected are not visible from the SSL VPN portal; however, users can still access the hidden pages unless you create SSL VPN access policies to prevent access to these pages.

4. Click **Apply** to save your settings. The new portal layout is added to the List of Layouts table. For information about how to display the new portal layout, see *Access the New SSL Portal Login Screen* on page 241.

- **To edit a portal layout:**

  1. On the Portal Layouts screen (see *Figure 132* on page 224), click the **Edit** button in the Action column for the portal layout that you want to modify. The Edit Portal Layout screen displays. This screen is identical to the Add Portal Layout screen (see the previous figure).
  2. Modify the settings as explained in the previous table.
  3. Click **Apply** to save your settings.

- **To delete one or more portal layouts:**

  1. On the Portal Layouts screen (see *Figure 132* on page 224), select the check box to the left of each portal layout that you want to delete, or click the **Select All** table button to select all layouts. (You cannot delete the SSL-VPN default portal layout.)
  2. Click the **Delete** table button.

Configure Domains, Groups, and Users

Remote users connecting to the wireless VPN firewall through an SSL VPN portal need to be authenticated before they are granted access to the network. The login screen that is presented to the user requires three items: a user name, a password, and a domain selection. The domain determines both the authentication method and the portal layout that are used.

You need to create name and password accounts for the SSL VPN users. When you create a user account, you need to specify a group. Groups are used to simplify the application of access policies. When you create a group, you need to specify a domain. Therefore, you should create any domains first, then groups, and then user accounts.

For information about how to configure domains, groups, and users, see *Configure Authentication Domains, Groups, and Users* on page 247.

Configure Applications for Port Forwarding

Port forwarding provides access to specific defined network services. To define these services, you need to specify the internal server addresses and port numbers for TCP applications that are intercepted by the port-forwarding client on the user's PC. This client reroutes the traffic to the wireless VPN firewall.

Add Servers and Port Numbers

To configure port forwarding, you need to define the IP addresses of the internal servers and the port number for TCP applications that are available to remote users.

➢ **To add a server and a port number:**

1. Select **VPN > SSL VPN > Port Forwarding**. The Port Forwarding screen displays. (The following figure shows an example.)

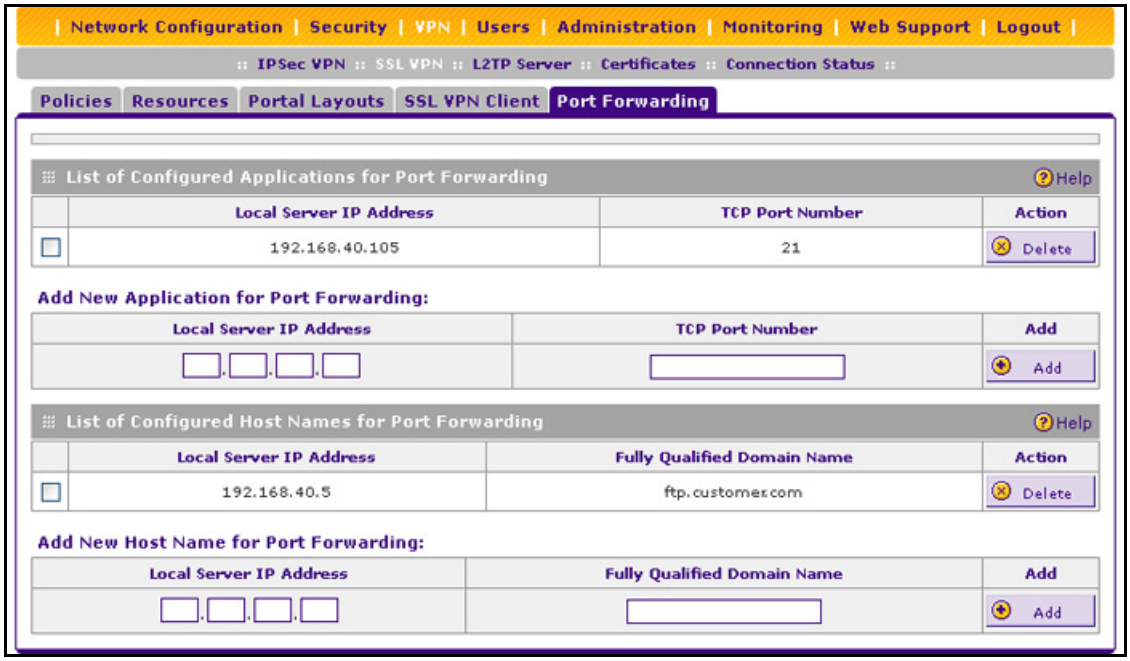


Figure 134.

2. In the Add New Application for Port Forwarding section of the screen, specify information in the following fields:
   - **IP Address**. The IP address of an internal server or host computer that a remote user has access to.
   - **TCP Port**. The TCP port number of the application that is accessed through the SSL VPN tunnel. The following table lists some commonly used TCP applications and port numbers.

Table 58. Port-forwarding applications/TCP port numbers

TCP Application	Port Number
FTP data (usually not needed)	20
FTP Control Protocol	21
SSH	22[a]
Telnet	23[a]
SMTP (send mail)	25
HTTP (web)	80
POP3 (receive mail)	110
NTP (Network Time Protocol)	123

Table 58. Port-forwarding applications/TCP port numbers (continued)

TCP Application	Port Number
Citrix	1494
Terminal Services	3389
VNC (virtual network computing)	5900 or 5800

a. Users can specify the port number together with the host name or IP address.

3. Click the **Add** table button. The new application entry is added to the List of Configured Applications for Port Forwarding table. Remote users can now securely access network applications once they have logged in to the SSL VPN portal and launched port forwarding.

➢ **To delete an application from the List of Configured Applications for Port Forwarding table:**

1. Select the check box to the left of the application that you want to delete.
2. Click the **Delete** table button in the Action column.

Add a New Host Name

After you have configured port forwarding by defining the IP addresses of the internal servers and the port number for TCP applications that are available to remote users, you then can also specify host-name-to-IP-address resolution for the network servers as a convenience for users. Host name resolution allows users to access TCP applications at familiar addresses such as mail.*example*.com or ftp.*customer*.com rather than by IP addresses.

➢ **To add servers and host names for client name resolution:**

1. Select **VPN > SSL VPN > Port Forwarding**. The Port Forwarding screen displays (see *Figure 134* on page 228).
2. In the Add New Host Name for Port Forwarding section of the screen, specify information in the following fields:
   - **Local Server IP Address**. The IP address of an internal server or host computer that you want to name.
   - **Fully Qualified Domain Name**. The full server name.

Note: If the server or host computer that you want to name does not display in the List of Configured Applications for Port Forwarding table, you need to add it before you can rename it.

3. Click the **Add** table button. The new application entry is added to the List of Configured Host Names for Port Forwarding table.

➢ **To delete a name from the List of Configured Host Names for Port Forwarding table:**

1. Select the check box to the left of the name that you want to delete.
2. Click the **Delete** table button in the Action column.

Configure the SSL VPN Client

The SSL VPN client on the wireless VPN firewall assigns IP addresses to remote VPN tunnel clients. Because the VPN tunnel connection is a point-to-point connection, you can assign IP addresses from the local subnet to the remote VPN tunnel clients.

The following are some additional considerations:

- So that the virtual (PPP) interface address of a VPN tunnel client does not conflict with addresses on the local network, configure an IP address range that does not directly overlap with addresses on your local network. For example, if 192.168.1.1 through 192.168.1.100 are currently assigned to devices on the local network, then start the client address range at 192.168.1.101, or choose an entirely different subnet altogether.
- The VPN tunnel client cannot contact a server on the local network if the VPN tunnel client's Ethernet interface shares the same IP address as the server or the wireless VPN firewall. (For example, if your PC has a network interface IP address of 10.0.0.45, then you cannot contact a server on the remote network that also has the IP address 10.0.0.45.)
- Select whether you want to enable full-tunnel or split-tunnel support based on your bandwidth:
  - A full tunnel sends all of the client's traffic across the VPN tunnel.
  - A split tunnel sends only traffic that is destined for the local network based on the specified client routes. All other traffic is sent to the Internet. A split tunnel allows you to manage bandwidth by reserving the VPN tunnel for local traffic only.
- If you enable split-tunnel support and you assign an entirely different subnet to the VPN tunnel clients from the subnet that is used by the local network, you need to add a client route to ensure that a VPN tunnel client connects to the local network over the VPN tunnel.

Configure the Client IP Address Range

First determine the address range to be assigned to VPN tunnel clients, and then define the address range.

➢ **To define the client IP address range:**

1. Select **VPN > SSL VPN > SSL VPN Client**. The SSL VPN Client screen displays:

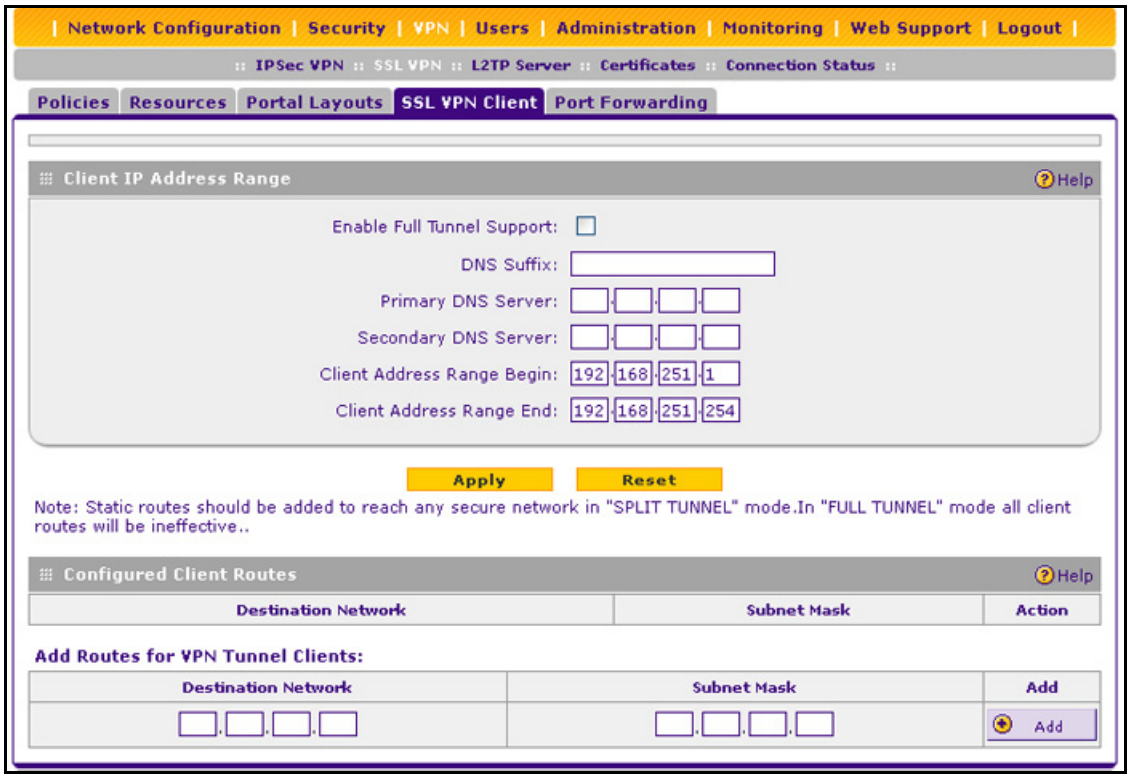

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
IPSec VPN :: SSL VPN :: L2TP Server :: Certificates :: Connection Status
Policies
Resources
Portal Layouts
SSL VPN Client
Port Forwarding
Client IP Address Range
Help
Enable Full Tunnel Support:
DNS Suffix:
Primary DNS Server:
Secondary DNS Server:
Client Address Range Begin: 192.168.251.1
Client Address Range End: 192.168.251.254
Apply
Reset
Note: Static routes should be added to reach any secure network in "SPLIT TUNNEL" mode.In "FULL TUNNEL" mode all client routes will be ineffective..
Configured Client Routes
Help
Destination Network
Subnet Mask
Action
Add Routes for VPN Tunnel Clients:
Destination Network
Subnet Mask
Add
Add

Figure 135.

2. Complete the settings as explained in the following table:

Table 59. SSL VPN Client screen settings

Setting	Description
Client IP Address Range	
Enable Full Tunnel Support	Select this check box to enable full-tunnel support. If you leave this check box cleared (which is the default setting), full-tunnel support is disabled but split-tunnel support is enabled, and you need to add client routes (see *Add Routes for VPN Tunnel Clients* on page 232). **Note:** When full-tunnel support is enabled, client routes are not operable.
DNS Suffix	A DNS suffix to be appended to incomplete DNS search strings. This setting is optional.
Primary DNS Server	The IP address of the primary DNS server that is assigned to the VPN tunnel clients. This setting is optional. **Note:** If you do not assign a DNS server, the DNS settings remain unchanged in the VPN client after a VPN tunnel has been established.
Secondary DNS Server	The IP address of the secondary DNS server that is assigned to the VPN tunnel clients. This setting is optional.

Table 59. SSL VPN Client screen settings (continued)

Setting	Description
Client Address Range Begin	The first IP address of the IP address range that you want to assign to the VPN tunnel clients. By default, the first IP address is 192.168.251.1.
Client Address Range End	The last IP address of the IP address range that you want to assign to the VPN tunnel clients. By default, the last IP address is 192.168.251.254.

3. Click **Apply** to save your settings. VPN tunnel clients are now able to connect to the wireless VPN firewall and receive a virtual IP address in the client address range.

Add Routes for VPN Tunnel Clients

The VPN tunnel clients assume that the following networks are located across the VPN-over-SSL tunnel:

- The subnet that contains the client IP address (that is, PPP interface), as determined by the class of the address (Class A, B, or C).
- Subnets that are specified in the Configured Client Routes table on the SSL VPN Client screen.

If the assigned client IP address range is in a different subnet from the local network, or if the local network has multiple subnets, or if you select split-tunnel operation, you need to define client routes.

➢ **To add an SSL VPN tunnel client route:**

1. Select **VPN > SSL VPN > SSL VPN Client**. The SSL VPN Client screen displays (see *Figure 135* on page 231).
2. In the Add Routes for VPN Tunnel Clients section of the screen, specify information in the following fields:
   - **Destination Network**. The destination network IP address of a local network or subnet. For example, enter 192.168.1.60.
   - **Subnet Mask**. The address of the appropriate subnet mask.
3. Click the **Add** table button. The new client route is added to the Configured Client Routes table.

If VPN tunnel clients are already connected, disconnect and then reconnect the clients on the SSL VPN Connection Status screen (see *View the SSL VPN Connection Status* on page 243). Doing so allows the clients to receive new addresses and routes.

➢ **To change the specifications of an existing route and to delete an old route:**

1. Add a new route to the Configured Client Routes table.
2. In the Configured Client Routes table, to the right of the route that is out-of-date, click the **Delete** table button.

If an existing route is no longer needed, you can delete it.

Use Network Resource Objects to Simplify Policies

Network resources are groups of IP addresses, IP address ranges, and services. By defining resource objects, you can more quickly create and configure network policies. You do not need to redefine the same set of IP addresses or address ranges when you configure the same access policies for multiple users.

Defining network resources is optional; smaller organizations can choose to create access policies using individual IP addresses or IP networks rather than predefined network resources. But for most organizations, NETGEAR recommends that you use network resources. If your server or network configuration changes, you can perform an update quickly by using network resources instead of individually updating all of the user and group policies.

Add New Network Resources

➢ **To define a network resource:**

1. Select **VPN > SSL VPN > Resources**. The Resources screen displays. (The following figure shows some resources in the List of Resources table as an example.)

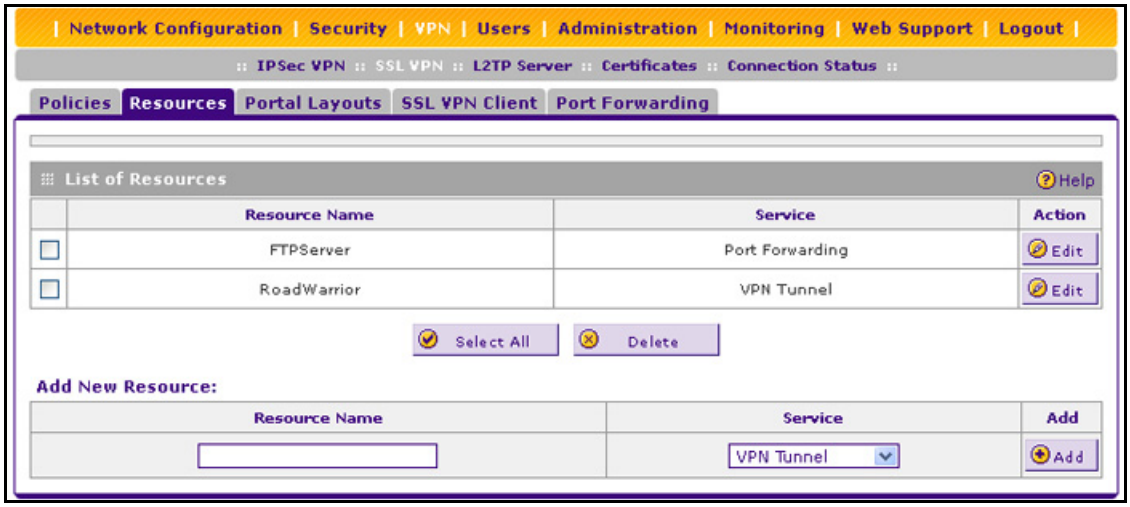


Figure 136.

2. In the Add New Resource section of the screen, specify information in the following fields:
   - **Resource Name**. A descriptive name of the resource for identification and management purposes.
   - **Service**. From the Service drop-down list, select the type of service to which the resource applies:
     - **VPN Tunnel**. The resource applies only to a VPN tunnel.
     - **Port Forwarding**. The resource applies only to port forwarding.
     - **All**. The resource applies both to a VPN tunnel and to port forwarding.
3. Click the **Add** table button. The new resource is added to the List of Resources table.

➢ **To delete one or more network resources:**

1. Select the check box to the left of each network resource that you want to delete, or click the **Select All** table button to select all network resources.
2. Click the **Delete** table button.

Edit Network Resources to Specify Addresses

➢ **To edit network resources:**

1. Select **VPN > SSL VPN > Resources**. The Resources screen displays (see the previous figure, which shows some examples).
2. In the List of Resources table, to the right of the new resource in the Action column, click the **Edit** table button. A new screen displays. (The following figure shows an example.)

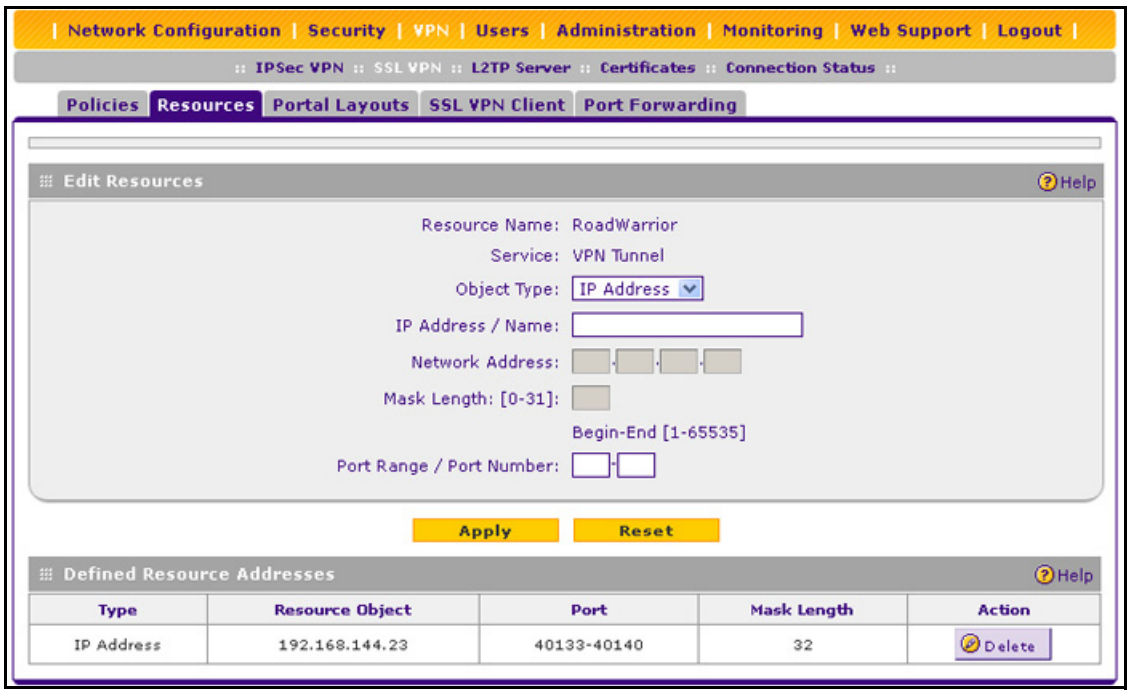


Figure 137.

3. Complete the settings as explained in the following table:

Table 60. Resources screen settings to edit a resource

Setting	Description
Add Resource Addresses	
Resource Name	The unique identifier for the resource. You cannot modify the resource name after you have created it on the first Resources screen.

Table 60. Resources screen settings to edit a resource (continued)

Setting	Description	
Service	The SSL service that is assigned to the resource. You cannot modify the service after you have assigned it to the resource on the first Resources screen.	
Object Type	From the drop-down list, select one of the following options: • **IP Address**. The object is an IP address. You need to enter the IP address or the FQDN in the IP Address / Name field. • **IP Network**. The object is an IP network. You need to enter the network IP address in the Network Address field and the network mask length in the Mask Length field.	
	IP Address / Name	Applicable only when you select IP Address as the object type. Enter the IP address or FQDN for the location that is permitted to use this resource.
	Network Address	Applicable only when you select IP Network as the object type. Enter the network IP address for the locations that are permitted to use this resource.
	Mask Length	Applicable only when you select IP Network as the object type. As an option, enter the network mask (0–31) for the locations that are permitted to use this resource.
Port Range / Port Number	A port or a range of ports (0–65535) to apply the policy to. The policy is applied to all TCP and UDP traffic that passes on those ports. Leave the fields blank to apply the policy to all traffic.	

4. Click **Apply** to save your settings. The new configuration is added to the Defined Resource Addresses table.

To delete a configuration from the Defined Resource Addresses table, click the **Delete** table button to the right of the configuration that you want to delete.

Configure User, Group, and Global Policies

You can define and apply user, group, and global policies to predefined network resource objects, IP addresses, address ranges, or all IP addresses, and to different SSL VPN services. A specific hierarchy is invoked over which policies take precedence. The wireless VPN firewall policy hierarchy is defined as follows:

- User policies take precedence over group policies.
- Group policies take precedence over global policies.
- If two or more user, group, or global policies are configured, the *most specific* policy takes precedence.

For example, a policy that is configured for a single IP address takes precedence over a policy that is configured for a range of addresses. And a policy that applies to a range of IP addresses takes precedence over a policy that is applied to all IP addresses. If two or more

IP address ranges are configured, then the smallest address range takes precedence. Host names are treated the same as individual IP addresses.

Network resources are prioritized just like other address ranges. However, the prioritization is based on the individual address or address range, not the entire network resource.

For example, assume the following global policy configuration:

- Policy 1. A Deny rule has been configured to block all services to the IP address range 10.0.0.0–10.0.0.255.
- Policy 2. A Deny rule has been configured to block FTP access to 10.0.1.2–10.0.1.10.
- Policy 3. A Permit rule has been configured to allow FTP access to the predefined network resource with the name FTP Servers. The FTP Servers network resource includes the following addresses: 10.0.0.5–10.0.0.20 and the FQDN ftp.*company*.com, which resolves to 10.0.1.3.

Assuming that no conflicting user or group policies have been configured, if a user attempted to access FTP servers at the following addresses, the actions listed would occur:

- 10.0.0.1. The user would be blocked by Policy 1.
- 10.0.1.5. The user would be blocked by Policy 2.
- 10.0.0.10. The user would be granted access by Policy 3. The IP address range 10.0.0.5–10.0.0.20 is more specific than the IP address range that is defined in Policy 1.
- ftp.*company*.com. The user would be granted access by Policy 3. A single host name is more specific than the IP address range that is configured in Policy 2.

Note: The user would not be able to access ftp.*company*.com using its IP address 10.0.1.3. The wireless VPN firewall's policy engine does not perform reverse DNS lookups.

View Policies

➢ **To view the existing policies:**

1. Select **VPN > SSL VPN**. The SSL VPN submenu tabs display, with the Policies screen in view. (The following figure shows some examples.)

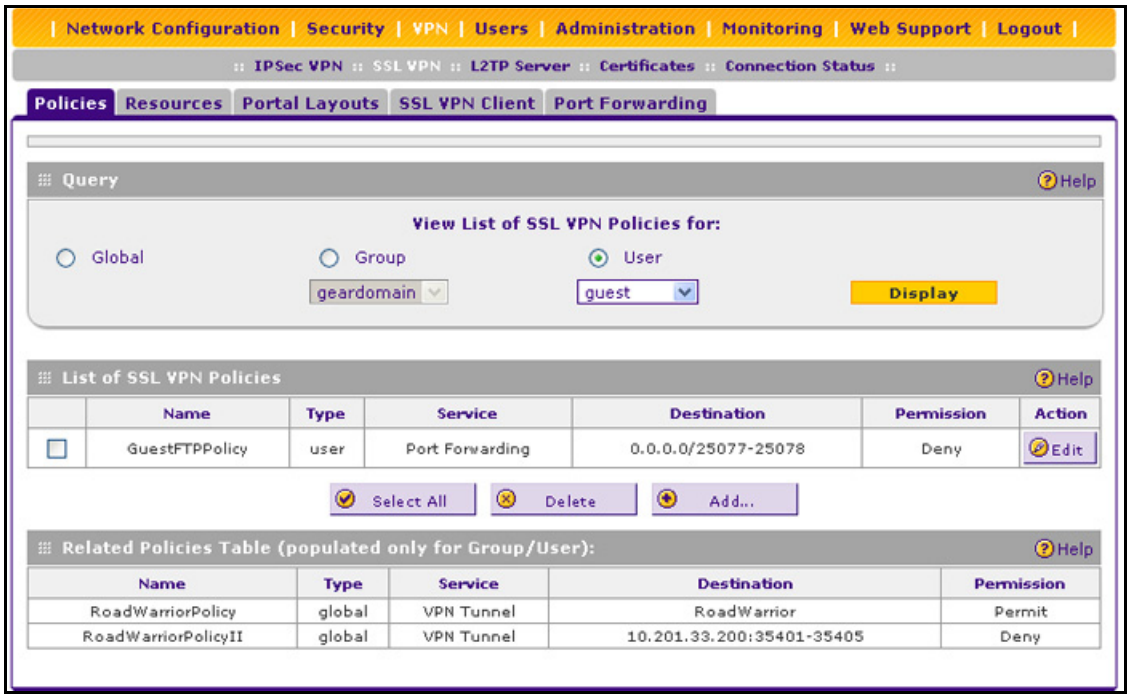

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
IPSec VPN :: SSL VPN :: L2TP Server :: Certificates :: Connection Status
Policies Resources Portal Layouts SSL VPN Client Port Forwarding
Query
Help
View List of SSL VPN Policies for:
Global
Group
User
geardomain
guest
Display
List of SSL VPN Policies
Help
Name Type Service Destination Permission Action
GuestFTPPolicy user Port Forwarding 0.0.0.0/25077-25078 Deny Edit
Select All
Delete
Add...
Related Policies Table (populated only for Group/User):
Help
Name Type Service Destination Permission
RoadWarriorPolicy global VPN Tunnel RoadWarrior Permit
RoadWarriorPolicyII global VPN Tunnel 10.201.33.200:35401-35405 Deny

Figure 138.

2. Make your selection from the following Query options:
   - To view all global policies, select the **Global** radio button.
   - To view group policies, select the **Group** radio button, and then select the relevant group's name from the drop-down list.
   - To view user policies, select the **User** radio button, and then select the relevant user's name from the drop-down list.
3. Click the **Display** action button. The List of SSL VPN Policies table displays the list for your selected Query option.

Add a Policy

➢ **To add an SSL VPN policy:**

1. Select **VPN > SSL VPN**. The SSL VPN submenu tabs display, with the Policies screen in view (see the previous figure).
2. Under the List of SSL VPN Policies table, click the **Add** table button. The Add SSL VPN Policy screen displays:

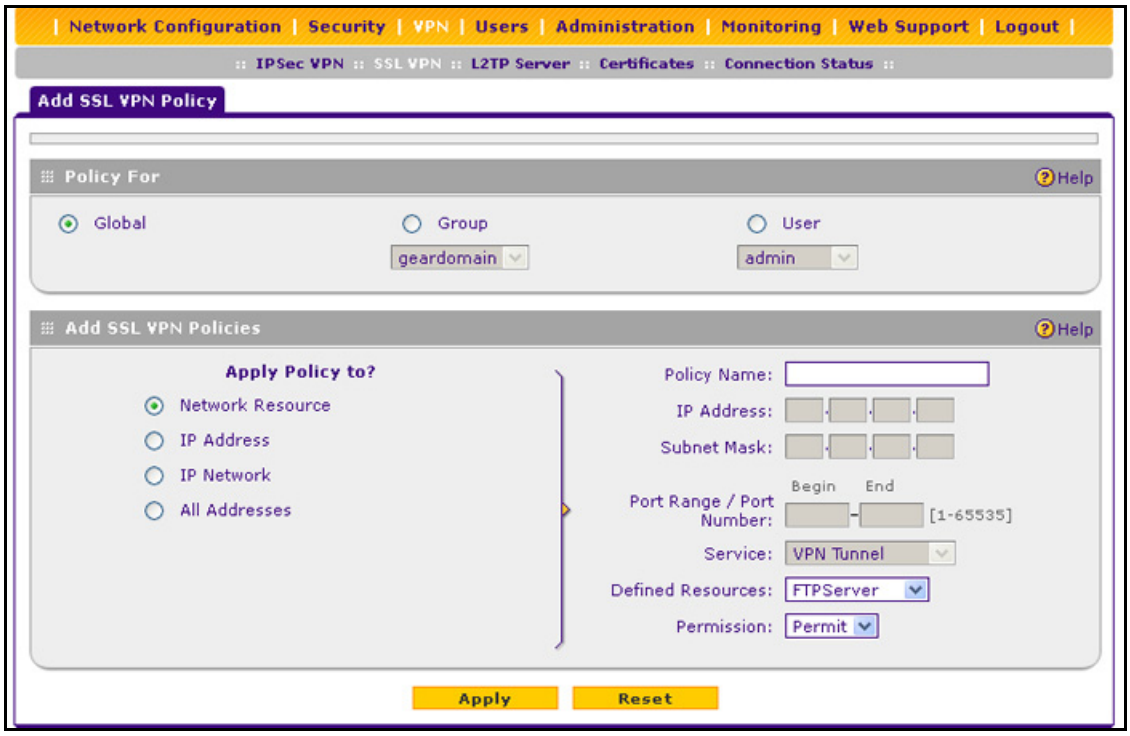


Figure 139.

3. Complete the settings as explained in the following table:

Table 61. Add SSL VPN Policy screen settings

Setting	Description
Policy For	
Select one of the following radio buttons to specify the type of SSL VPN policy: • **Global**. The new policy is global and includes all groups and users. • **Group**. The new policy needs to be limited to a single group. From the drop-down list, select a group name. For information about how to create groups, see *Configure Groups* on page 251. • **User**. The new policy needs to be limited to a single user. From the drop-down list, select a user name. For information about how to create user accounts, see *Configure User Accounts* on page 254.	
Add SSL VPN Policies	
Apply Policy to?	Select one of the following radio buttons to specify how the policy is applied. When you select a radio button, the fields and drop-down lists that apply to your selection (see explanations later in this table) unmask onscreen. • **Network Resource**. The policy is applied to a network resource that you have defined on the Resources screen (see *Use Network Resource Objects to Simplify Policies* on page 233). • **IP Address**. The policy is applied to a single IP address. • **IP Network**. The policy is applied to a network address. • **All Addresses**. The policy is applied to all addresses.

Table 61. Add SSL VPN Policy screen settings (continued)

Setting	Description		
Apply Policy to? (continued)	Network Resource	Policy Name	A descriptive name of the SSL VPN policy for identification and management purposes.
		Defined Resources	From the drop-down list, select a network resource that you have defined on the Resources screen (see *Use Network Resource Objects to Simplify Policies* on page 233).
		Permission	From the drop-down list, select **Permit** or **Deny** to specify whether the policy permits or denies access.
	IP Address	Policy Name	A descriptive name of the SSL VPN policy for identification and management purposes.
		IP Address	The IP address to which the SSL VPN policy is applied.
		Port Range / Port Number	A port (fill in the Begin field) or a range of ports (fill in the Begin and End fields) to which the SSL VPN policy is applied. Ports can be 0 through 65535. The policy is applied to all TCP and UDP traffic that passes on those ports. Leave the fields blank to apply the policy to all traffic.
		Service	From the drop-down list, select the service to which the SSL VPN policy is applied: • **VPN Tunnel**. The policy is applied only to a VPN tunnel. • **Port Forwarding**. The policy is applied only to port forwarding. • **All**. The policy is applied both to a VPN tunnel and to port forwarding.
		Permission	From the drop-down list, select **Permit** or **Deny** to specify whether the policy permits or denies access.
	IP Network	Policy Name	A descriptive name of the SSL VPN policy for identification and management purposes.
		IP Address	The network IP address to which the SSL VPN policy is applied.
		Subnet Mask	The network subnet mask to which the SSL VPN policy is applied.
		Port Range / Port Number	A port (fill in the Begin field) or a range of ports (fill in the Begin and End fields) to which the SSL VPN policy is applied. Ports can be 0 through 65535. The policy is applied to all TCP and UDP traffic that passes on those ports. Leave the fields blank to apply the policy to all traffic.

Table 61. Add SSL VPN Policy screen settings (continued)

Setting	Description		
Apply Policy to? (continued)	IP Network (continued)	Service	From the drop-down list, select the service to which the SSL VPN policy is applied: • **VPN Tunnel**. The policy is applied only to a VPN tunnel. • **Port Forwarding**. The policy is applied only to port forwarding. • **All**. The policy is applied both to a VPN tunnel and to port forwarding.
		Permission	From the drop-down list, select **Permit** or **Deny** to specify whether the policy permits or denies access.
	All Addresses	Policy Name	A descriptive name of the SSL VPN policy for identification and management purposes.
		Port Range / Port Number	A port (fill in the Begin field) or a range of ports (fill in the Begin and End fields) to which the SSL VPN policy is applied. Ports can be 0 through 65535. The policy is applied to all TCP and UDP traffic that passes on those ports. Leave the fields blank to apply the policy to all traffic.
		Service	From the drop-down list, select the service to which the SSL VPN policy is applied: • **VPN Tunnel**. The policy is applied only to a VPN tunnel. • **Port Forwarding**. The policy is applied only to port forwarding. • **All**. The policy is applied both to a VPN tunnel and to port forwarding.
		Permission	From the drop-down list, select **Permit** or **Deny** to specify whether the policy permits or denies access.

4. Click **Apply** to save your settings. The policy is added to the List of SSL VPN Policies table on the Policies screen. The new policy goes into effect immediately.

Note: If you have configured SSL VPN user policies, make sure that secure HTTP remote management is enabled (see *Configure Remote Management Access* on page 278). If secure HTTP remote management is not enabled, all SSL VPN user connections are disabled.

➢ **To edit an SSL VPN policy:**

1. On the Policies screen (see *Figure 138* on page 237), click the **Edit** button in the Action column for the SSL VPN policy that you want to modify. The Edit SSL VPN Policy screen displays. This screen is identical to the Add SSL VPN Policy screen (see previous screen).
2. Modify the settings as explained in the previous table.
3. Click **Apply** to save your settings.

➢ **To delete one or more SSL VPN policies:**

1. On the Policies screen (see *Figure 138* on page 237), select the check box to the left of each SSL VPN policy that you want to delete, or click the **Select All** table button to select all policies.
2. Click the **Delete** table button.

Access the New SSL Portal Login Screen

All screens that you can access from the SSL VPN menu of the web management interface display a user portal link in the upper right of the screen, above the menu bars (User Portal).

When you click the **User Portal** link, the SSL VPN default portal opens (see *Figure 141* on page 242). This user portal is not the same as the new SSL portal login screen that you defined with the help of the SSL VPN Wizard.

➢ **To open the new SSL portal login screen:**

1. Select **VPN > SSL VPN > Portal Layouts**. The Portal Layouts screen displays (see *Figure 132* on page 224).
2. In the Portal URL field of the List of Layouts table, select the URL that ends with the portal layout name that you defined with the help of the SSL VPN Wizard. The new SSL portal login screen displays:

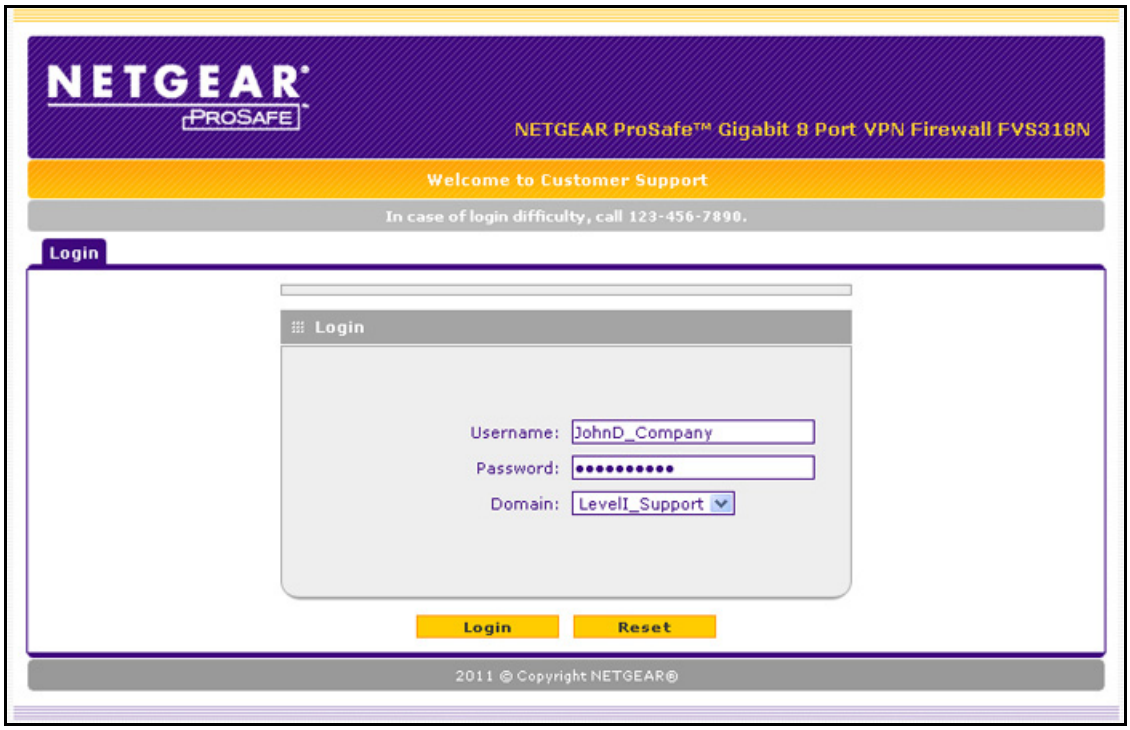


Figure 140.

3. Enter the user name and password that you just created with the help of the SSL VPN Wizard.

4. Click **Login**. The User Portal screen displays. The format of the User Portal screen depends on the settings that you selected on the Add Portal Layout screen (see *Create the Portal Layout* on page 223):
   - *Figure 141* shows the User Portal screen with both a VPN Tunnel and a Port Forwarding menu option.
   - *Figure 142* show the User Portal screen with a Port Forwarding menu option only. The VPN Tunnel menu option is not displayed.

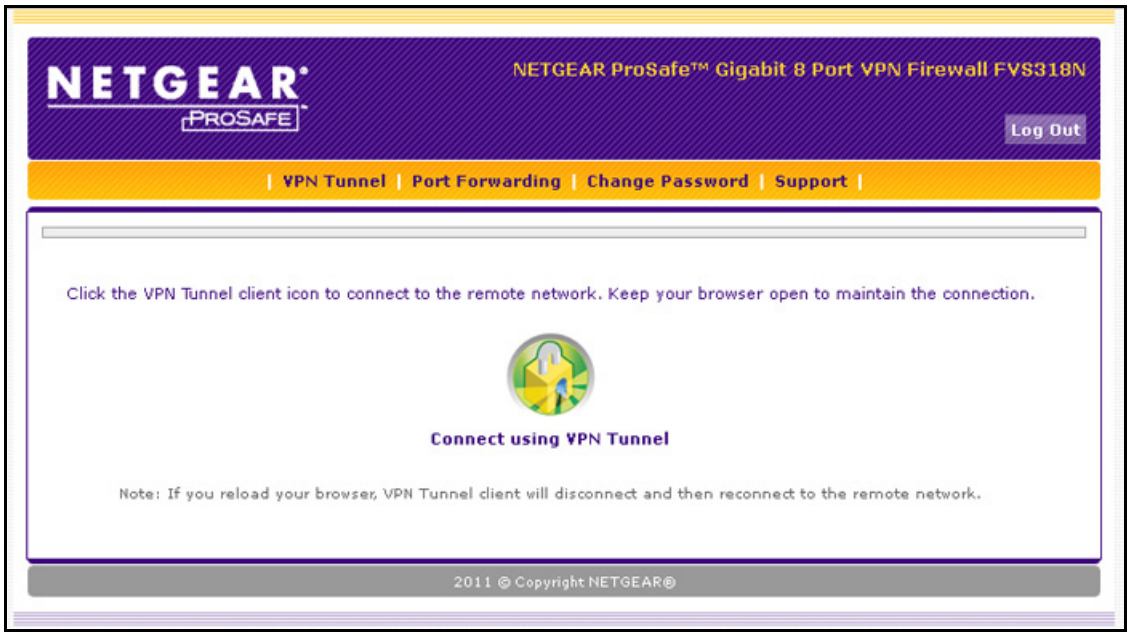

NETGEAR
PROSAFE
NETGEAR ProSafe™ Gigabit 8 Port VPN Firewall FVS318N
Log Out
| VPN Tunnel | Port Forwarding | Change Password | Support |
Click the VPN Tunnel client icon to connect to the remote network. Keep your browser open to maintain the connection.
Connect using VPN Tunnel
Note: If you reload your browser, VPN Tunnel client will disconnect and then reconnect to the remote network.
2011 © Copyright NETGEAR®

Figure 141.

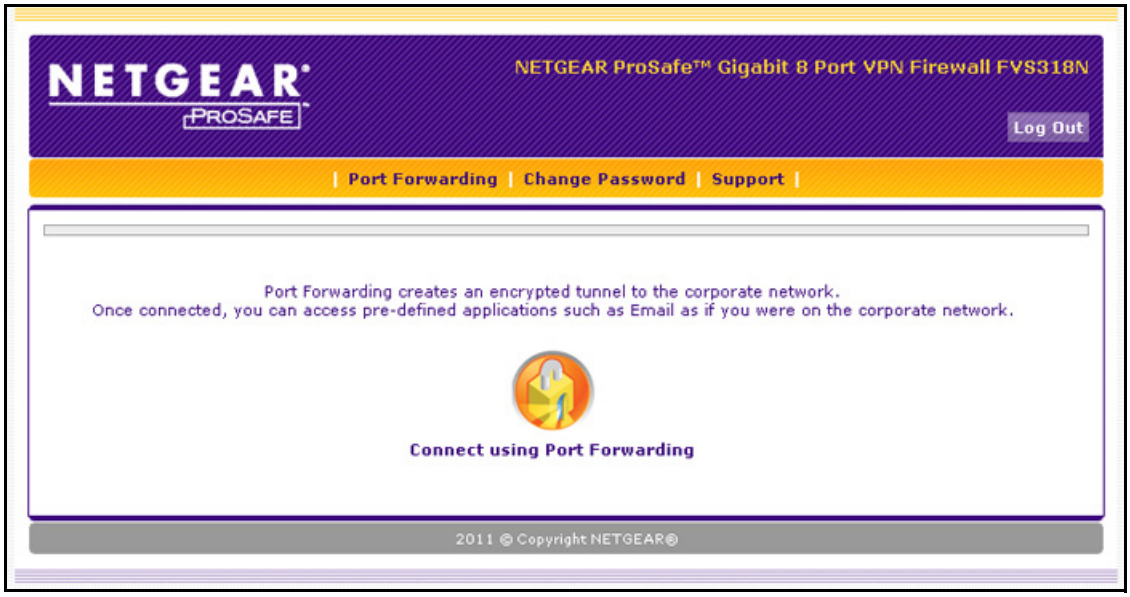

NETGEAR
PROSAFE
NETGEAR ProSafe™ Gigabit 8 Port VPN Firewall FVS318N
Log Out
| Port Forwarding | Change Password | Support |
Port Forwarding creates an encrypted tunnel to the corporate network.
Once connected, you can access pre-defined applications such as Email as if you were on the corporate network.
Connect using Port Forwarding
2011 © Copyright NETGEAR®

Figure 142.

The User Portal screen displays a simple menu that, depending on the resources allocated, provides the SSL user with the following menu selections:

- **VPN Tunnel**. Provides full network connectivity.
- **Port Forwarding**. Provides access to the network services that you defined as described in *Configure Applications for Port Forwarding* on page 227.
- **Change Password**. Allows the user to change his or her password.
- **Support**. Provides access to the NETGEAR website.

Note: The first time that a user attempts to connect through the VPN tunnel, the NETGEAR SSL VPN tunnel adapter is installed; the first time that a user attempts to connect through the port-forwarding tunnel, the NETGEAR port-forwarding engine is installed.

View the SSL VPN Connection Status

To view the status of current SSL VPN tunnels, select **VPN > Connection Status > SSL VPN Connection Status**. The SSL VPN Connection Status screen displays:

Figure 143.

The active user's name, group, and IP address are listed in the table with a time stamp indicating the time and date that the user connected.

To disconnect an active user, click the **Disconnect** table button to the right of the user's table entry.

View the SSL VPN Log

➢ **To display the SSL VPN log:**

Select **Monitoring > VPN Logs > SSL VPN Logs.** The SSL VPN Logs screen displays:

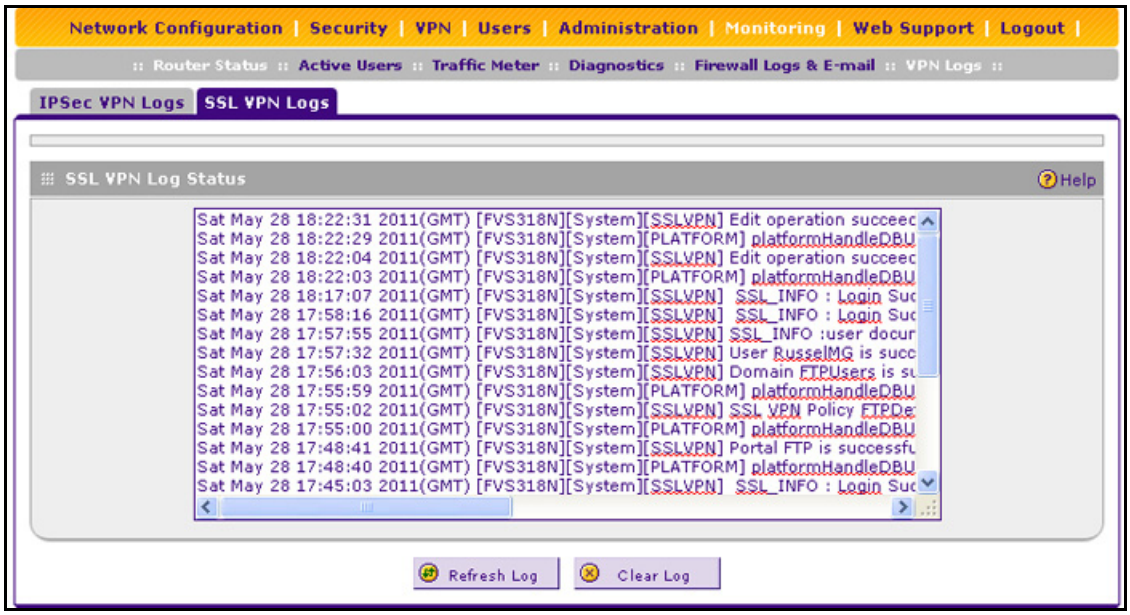

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Router Status :: Active Users :: Traffic Meter :: Diagnostics :: Firewall Logs & E-mail :: VPN Logs ::
IPSec VPN Logs
SSL VPN Logs
SSL VPN Log Status
Help
Sat May 28 18:22:31 2011(GMT) [FVS318N][System][SSLVPN] Edit operation succeec
Sat May 28 18:22:29 2011(GMT) [FVS318N][System][PLATFORM] platformHandleDBU
Sat May 28 18:22:04 2011(GMT) [FVS318N][System][SSLVPN] Edit operation succeec
Sat May 28 18:22:03 2011(GMT) [FVS318N][System][PLATFORM] platformHandleDBU
Sat May 28 18:17:07 2011(GMT) [FVS318N][System][SSLVPN] SSL_INFO : Login Suc
Sat May 28 17:58:16 2011(GMT) [FVS318N][System][SSLVPN] SSL_INFO : Login Suc
Sat May 28 17:57:55 2011(GMT) [FVS318N][System][SSLVPN] SSL_INFO :user docur
Sat May 28 17:57:32 2011(GMT) [FVS318N][System][SSLVPN] User RusselMG is succ
Sat May 28 17:56:03 2011(GMT) [FVS318N][System][SSLVPN] Domain FTPUsers is su
Sat May 28 17:55:59 2011(GMT) [FVS318N][System][PLATFORM] platformHandleDBU
Sat May 28 17:55:02 2011(GMT) [FVS318N][System][SSLVPN] SSL VPN Policy FTPDe
Sat May 28 17:55:00 2011(GMT) [FVS318N][System][PLATFORM] platformHandleDBU
Sat May 28 17:48:41 2011(GMT) [FVS318N][System][SSLVPN] Portal FTP is successfu
Sat May 28 17:48:40 2011(GMT) [FVS318N][System][PLATFORM] platformHandleDBU
Sat May 28 17:45:03 2011(GMT) [FVS318N][System][SSLVPN] SSL_INFO : Login Suc
Refresh Log
Clear Log

Figure 144.

Manage Users, Authentication, and VPN Certificates

8

This chapter describes how to manage users, authentication, and security certificates for IPSec VPN and SSL VPN. This chapter contains the following sections:

- *The Wireless VPN Firewall's Authentication Process and Options*
- *Configure Authentication Domains, Groups, and Users*
- *Manage Digital Certificates for VPN Connections*

The Wireless VPN Firewall's Authentication Process and Options

Users are assigned to a group, and a group is assigned to a domain. Therefore, you should first create any domains, then groups, then user accounts.

> **Note:** Do not confuse the authentication groups with the LAN groups that are discussed in *Manage IPv4 Groups and Hosts (IPv4 LAN Groups)* on page 59.

You need to create name and password accounts for all users who need to be able to connect to the wireless VPN firewall. This includes administrators, guests, and SSL VPN clients. Accounts for IPSec VPN clients are required only if you have enabled extended authentication (XAUTH) in your IPSec VPN configuration.

Users connecting to the wireless VPN firewall need to be authenticated before being allowed to access the wireless VPN firewall or the VPN-protected network. The login screen that is presented to the user requires three items: a user name, a password, and a domain selection. The domain determines the authentication method that is used and, for SSL connections, the portal layout that is presented.

> **Note:** IPSec VPN users always belong to the default domain (geardomain) and are not assigned to groups.

Except in the case of IPSec VPN users, when you create a user account, you need to specify a group. When you create a group, you need to specify a domain.

The following table summarizes the external authentication protocols and methods that the wireless VPN firewall supports.

Table 62. External authentication protocols and methods

Authentication protocol or method	Description
PAP	Password Authentication Protocol (PAP) is a simple protocol in which the client sends a password in clear text.
CHAP	Challenge Handshake Authentication Protocol (CHAP) executes a three-way handshake in which the client and server trade challenge messages, each responding with a hash of the other's challenge message that is calculated using a shared secret value.
RADIUS	A network-validated PAP or CHAP password-based authentication method that functions with Remote Authentication Dial In User Service (RADIUS).
MIAS	A network-validated PAP or CHAP password-based authentication method that functions with Microsoft Internet Authentication Service (MIAS), which is a component of Microsoft Windows 2003 Server.
WiKID	WiKID Systems is a PAP or CHAP key-based two-factor authentication method that functions with public key cryptography. The client sends an encrypted PIN to the WiKID server and receives a one-time passcode with a short expiration period. The client logs in with the passcode. See *Appendix B, Two-Factor Authentication*, for more on WiKID authentication.
NT Domain	A network-validated domain-based authentication method that functions with a Microsoft Windows NT Domain authentication server. This authentication method has been superseded by Microsoft Active Directory authentication but is supported to authenticate legacy Windows clients.
Active Directory	A network-validated domain-based authentication method that functions with a Microsoft Active Directory authentication server. Microsoft Active Directory authentication servers support a group and user structure. Because the Active Directory supports a multilevel hierarchy (for example, groups or organizational units), this information can be queried to provide specific group policies or bookmarks based on Active Directory attributes. **Note:** A Microsoft Active Directory database uses an LDAP organization schema.
LDAP	A network-validated domain-based authentication method that functions with a Lightweight Directory Access Protocol (LDAP) authentication server. LDAP is a standard for querying and updating a directory. Because LDAP supports a multilevel hierarchy (for example, groups or organizational units), this information can be queried to provide specific group policies or bookmarks based on LDAP attributes.

Configure Authentication Domains, Groups, and Users

This section contains the following subsections:

- *Configure Domains*
- *Configure Groups*
- *Configure User Accounts*
- *Set User Login Policies*
- *Change Passwords and Other User Settings*

Configure Domains

The domain determines the authentication method to be used for associated users. For SSL connections, the domain also determines the portal layout that is presented, which in turn determines the network resources to which the associated users have access. The default domain of the wireless VPN firewall is named geardomain. You cannot delete the default domain.

Create Domains

➢ **To create a domain:**

1. Select **Users > Domains**. The Domains screen displays. (The following figure shows the wireless VPN firewall's default domain—geardomain—and, as an example, other domains in the List of Domains table.)

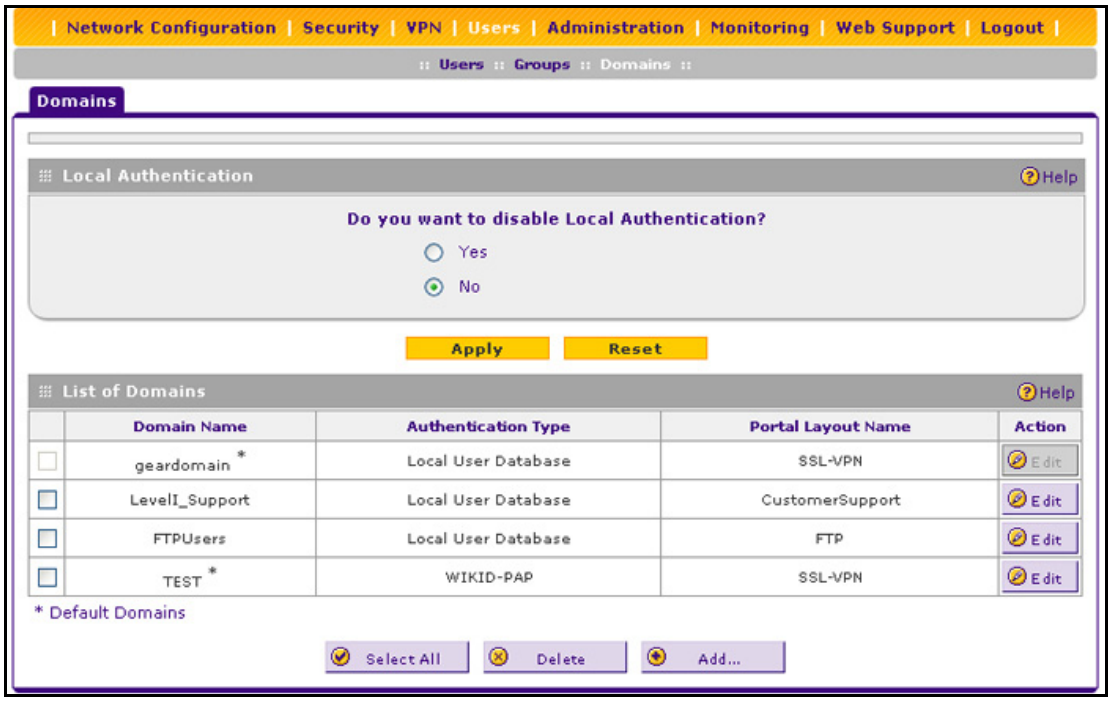


Figure 145.

The List of Domains table displays the domains with the following fields:

- **Check box**. Allows you to select the domain in the table.
- **Domain Name**. The name of the domain. The name of the default domain (geardomain) to which the default SSL-VPN portal is assigned is appended by an asterisk. The name of any other domain to which the default SSL-VPN portal is assigned is also appended by an asterisk (TEST in the previous figure).
- **Authentication Type**. The authentication method that is assigned to the domain.
- **Portal Layout Name**. The SSL portal layout that is assigned to the domain.
- **Action**. The Edit table button, which provides access to the Edit Domain screen.

2. Under the List of Domains table, click the **Add** table button. The Add Domain screen displays:

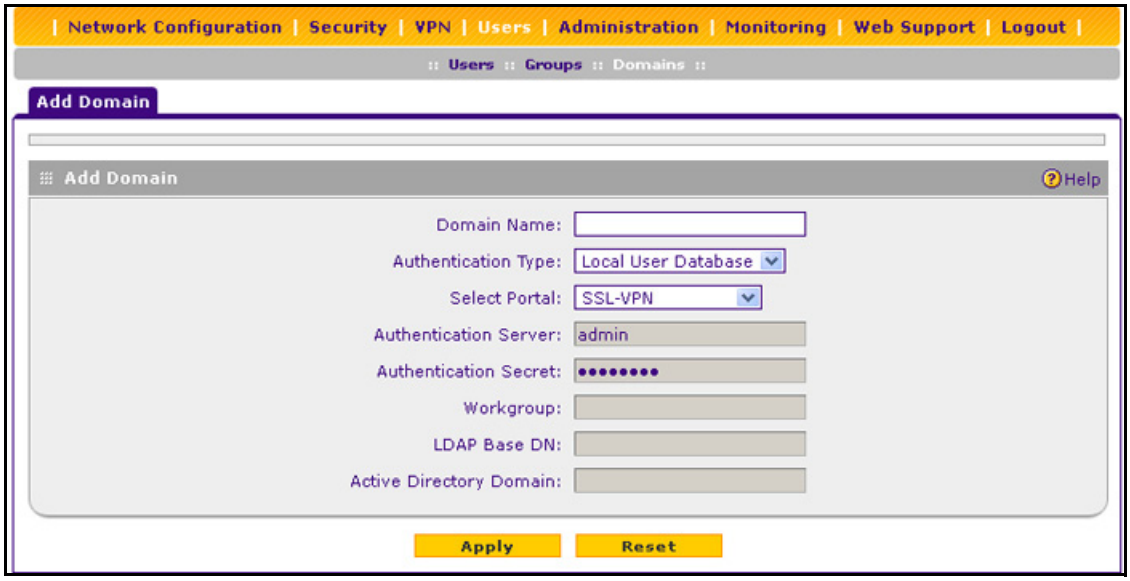


Figure 146.

3. Complete the settings as explained in the following table:

Table 63. Add Domain screen settings

Setting	Description
Domain Name	A descriptive (alphanumeric) name of the domain for identification and management purposes.
Authentication Type	From the drop-down list, select the authentication method that the wireless VPN firewall applies: • **Local User Database (default)**. Users are authenticated locally on the wireless VPN firewall. This is the default setting. You do not need to complete any other fields on this screen. • **Radius-PAP**. RADIUS Password Authentication Protocol (PAP). Complete the following fields: - Authentication Server - Authentication Secret

Table 63. Add Domain screen settings (continued)

Setting	Description
Authentication Type (continued) **Note:** If you select any type of RADIUS authentication, make sure that one or more RADIUS servers are configured (see *RADIUS Client Configuration* on page 196).	• **Radius-CHAP**. RADIUS Challenge Handshake Authentication Protocol (CHAP). Complete the following fields: - Authentication Server - Authentication Secret • **Radius-MSCHAP**. RADIUS Microsoft CHAP. Complete the following fields: - Authentication Server - Authentication Secret • **Radius-MSCHAPv2**. RADIUS Microsoft CHAP version 2. Complete the following fields: - Authentication Server - Authentication Secret • **WIKID-PAP**. WiKID Systems PAP. Complete the following fields: - Authentication Server - Authentication Secret • **WIKID-CHAP**. WiKID Systems CHAP. Complete the following fields: - Authentication Server - Authentication Secret • **MIAS-PAP**. Microsoft Internet Authentication Service (MIAS) PAP. Complete the following fields: - Authentication Server - Authentication Secret • **MIAS-CHAP**. Microsoft Internet Authentication Service (MIAS) CHAP. Complete the following fields: - Authentication Server - Authentication Secret • **NT Domain**. Microsoft Windows NT Domain. Complete the following fields: - Authentication Server - Workgroup • **Active Directory**. Microsoft Active Directory. Complete the following fields, and make a selection from the LDAP Encryption drop-down list: - Authentication Server - Active Directory Domain • **LDAP**. Lightweight Directory Access Protocol (LDAP). Complete the following fields, and make a selection from the LDAP Encryption drop-down list: - Authentication Server - LDAP Base DN
Select Portal	The portal that is assigned to this domain and that is presented to the user to enter credentials. The default portal is SSL-VPN.
Authentication Server	The server IP address or server name of the authentication server for any type of authentication other than authentication through the local user database.
Authentication Secret	The authentication secret or password that is required to access the authentication server for RADIUS, WiKID, or MIAS authentication.
Workgroup	The workgroup that is required for Microsoft NT Domain authentication.

Table 63. Add Domain screen settings (continued)

Setting	Description
LDAP Base DN	The LDAP distinguished name (DN) that is required to access the LDAP authentication server. This should be a user in the LDAP directory who has read access to all the users that you would like to import into the wireless VPN firewall. The Bind DN field accepts two formats: • **A display name in the DN format**. For example: cn=Jamie Hanson,cn=users,dc=test,dc=com. • **A Windows login account name in email format**. For example: jhanson@testAD.com. This last type of bind DN can be used only for a Windows LDAP server.
Active Directory Domain	The Active Directory domain name that is required for Microsoft Active Directory authentication.

4. Click **Apply** to save your settings. The domain is added to the List of Domains table.
5. If you use local authentication, make sure that it is not disabled: in the Local Authentication section of the Domain screen (see *Figure 145* on page 247), select the **No** radio button.

Note: A combination of local and external authentication is supported.

WARNING!

If you disable local authentication, make sure that there is at least one external administrative user; otherwise, access to the wireless VPN firewall is blocked.

6. If you do change local authentication, click **Apply** in the Domain screen to save your settings.

➢ **To delete one or more domains:**

1. In the List of Domains table, select the check box to the left of each domain that you want to delete, or click the **Select All** table button to select all domains.
2. Click the **Delete** table button.

Note: You cannot delete the geardomain default domain.

Edit Domains

➢ **To edit a domain:**

1. Select **Users > Domains**. The Domains screen displays (see *Figure 145* on page 247).
2. In the Action column of the List of Domains table, click the **Edit** table button for the domain that you want to edit. The Edit Domains screen displays. This screen is very similar to the Add Domains screen (see the previous figure).
3. Modify the settings as explained in the previous table. (You cannot modify the Domain Name and Authentication Type fields.)
4. Click **Apply** to save your changes. The modified domain is displayed in the List of Domains table.

Note: You cannot edit the geardomain default domain.

Configure Groups

The use of groups simplifies the configuration of VPN policies when different sets of users have different restrictions and access controls. It also simplifies the configuration of web access exception rules. Like the default domain of the wireless VPN firewall, the default group is also named geardomain. The default group geardomain is assigned to the default domain geardomain. You cannot delete the default domain geardomain, nor its associated default group geardomain.

IMPORTANT:

When you create a new domain on the Domains screen (see the previous section), a default group with the same name as the new domain is created automatically. The name of a default group is appended by an asterisk, and you cannot delete a default group. However, when you delete the domain with which it is associated, the default group is deleted automatically.

Note: IPSec VPN users always belong to the default domain (geardomain) and are not assigned to groups.

Note: Groups that are defined on the Groups screen are used for setting SSL VPN policies. These groups should not be confused with LAN groups that are defined on the IPv4 LAN Groups screen and that are used to simplify firewall policies. For information about LAN groups, see *Manage IPv4 Groups and Hosts (IPv4 LAN Groups)* on page 59.

Create Groups

➢ **To create a VPN group:**

1. Select **Users > Groups**. The Groups screen displays. (The following figure shows the wireless VPN firewall's default group—geardomain—and, as an example, several other groups in the List of Groups table.)

   The List of Groups table displays the VPN groups with the following fields:

   - **Check box**. Allows you to select the group in the table.
   - **Name**. The name of the group. If the group name is appended by an asterisk, the group was created by default when you created the domain with the identical name as the default group. You cannot delete a default group; you can delete only the domain with the identical name, which causes the default group to be deleted.
   - **Domain**. The name of the domain to which the group is assigned.
   - **Action**. The Edit table button, which provides access to the Edit Group screen.

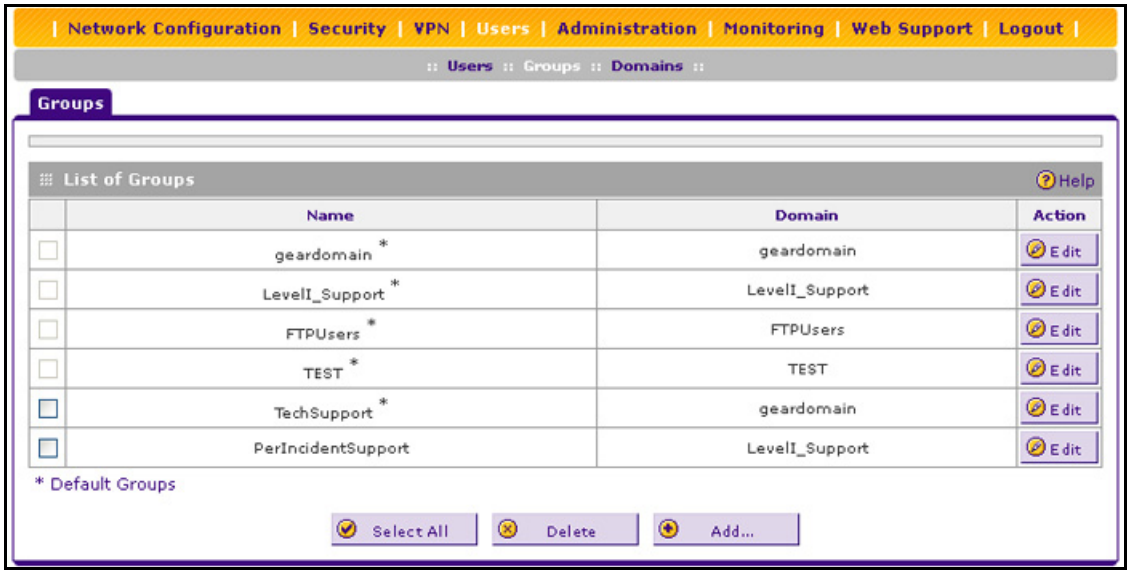


Figure 147.

2. Under the List of Groups table, click the **Add** table button. The Add Group screen displays:

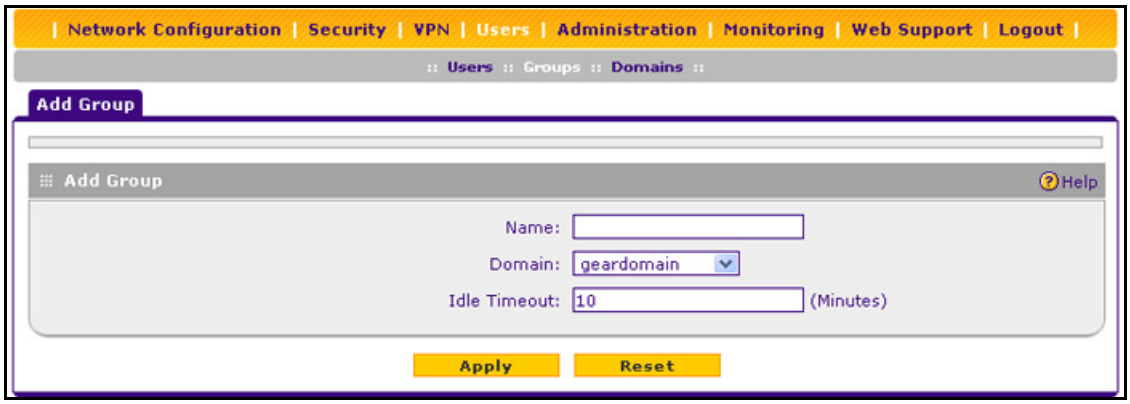


Figure 148.

3. Complete the settings as explained in the following table:

Table 64. Add Group screen settings

Setting	Description
Name	A descriptive (alphanumeric) name of the group for identification and management purposes.
Domain	The drop-down list shows the domains that are listed on the Domain screen. From the drop-down list, select the domain with which the group is associated. For information about how to configure domains, see *Configure Domains* on page 247.
Idle Timeout	The period after which an idle user is automatically logged out of the wireless VPN firewall's web management interface. The default idle time-out period is 10 minutes.

4. Click **Apply** to save your changes. The new group is added to the List of Groups table.

➢ **To delete one or more groups:**

1. In the List of Groups table, select the check box to the left of each group that you want to delete, or click the **Select All** table button to select all groups.
2. Click the **Delete** table button.

Note: You can delete only groups that you created on the Groups screen. Groups that were automatically created when you created a domain cannot be deleted on the Groups screen. See the Important note at the beginning of this section.

Edit Groups

For groups that were automatically created when you created a domain, you can modify only the idle time-out settings but not the group name or associated domain.

For groups that you created on the Add Groups screen, you can modify the domain and the idle time-out settings but not the group name.

➢ **To edit a VPN group:**

1. Select **Users > Groups**. The Groups screen displays (see *Figure 147* on page 252).
2. In the Action column of the List of Groups table, click the **Edit** table button for the group that you want to edit. The Edit Groups screen displays. This screen is identical to the Add Groups screen.
3. Modify the settings as explained in the previous table.
4. Click **Apply** to save your changes. The modified group is displayed in the List of Groups table.

Configure User Accounts

When you create a user account, you need to assign the user to a user group. When you create a group, you need to assign the group to a domain that specifies the authentication method. Therefore, you should first create any domains, then groups, and then user accounts.

Note: IPSec VPN users always belong to the default domain (geardomain) and default group (also geardomain) and do not need to be assigned a user account.

There are two default user accounts:

- A user with the name **admin** and the password **password**. This is a user who has read/write access, is associated with the domain geardomain, and is denied login from the WAN interface by default. The user name is appended by an asterisk. You cannot delete this user account.
- A user with the name **guest** and the password **password**. This is a user who has read-only access, is associated with the domain geardomain, and is denied login from the WAN interface by default. The user name is appended by an asterisk. You cannot delete this user account.

You can create five different types of user accounts by applying one of the predefined user types:

- **SSL VPN user**. A user who can log in only to the SSL VPN portal.
- **Administrator**. A user who has full access and the capacity to change the wireless VPN firewall configuration (that is, read-write access).
- **Guest user**. A user who can only view the wireless VPN firewall configuration (that is, read-only access).
- **IPSec VPN user**. A user who can make an IPSec VPN connection only through a NETGEAR ProSafe VPN Client, and only when the XAUTH feature is enabled (see *Configure Extended Authentication (XAUTH)* on page 194).
- **L2TP user**. A user who can connect over an L2TP connection to an L2TP client that is located behind the wireless VPN firewall.

➢ **To create a user account:**

1. Select **Users > Users**. The Users screen displays. (The following figure shows the wireless VPN firewall's default users—admin and guest—and, as an example, several other users in the List of Users table.)

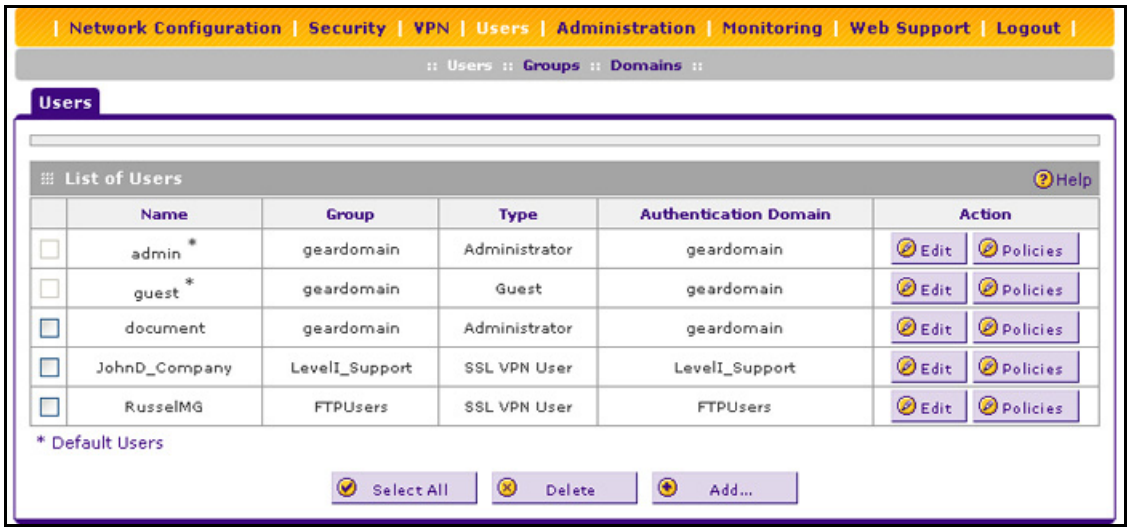


Figure 149.

The List of Users table displays the users and has the following fields:

- **Check box**. Allows you to select the user in the table.
- **Name**. The name of the user. If the user name is appended by an asterisk, the user is a default user that came preconfigured with the wireless VPN firewall and cannot be deleted.
- **Group**. The group to which the user is assigned.
- **Type**. The type of access credentials that are assigned to the user.
- **Authentication Domain**. The authentication domain to which the user is assigned.
- **Action**. The Edit table button, which provides access to the Edit User screen; the Policies table button, which provides access to the policy screens.

2. Under the List of Users table, click the **Add** table button. The Add User screen displays:

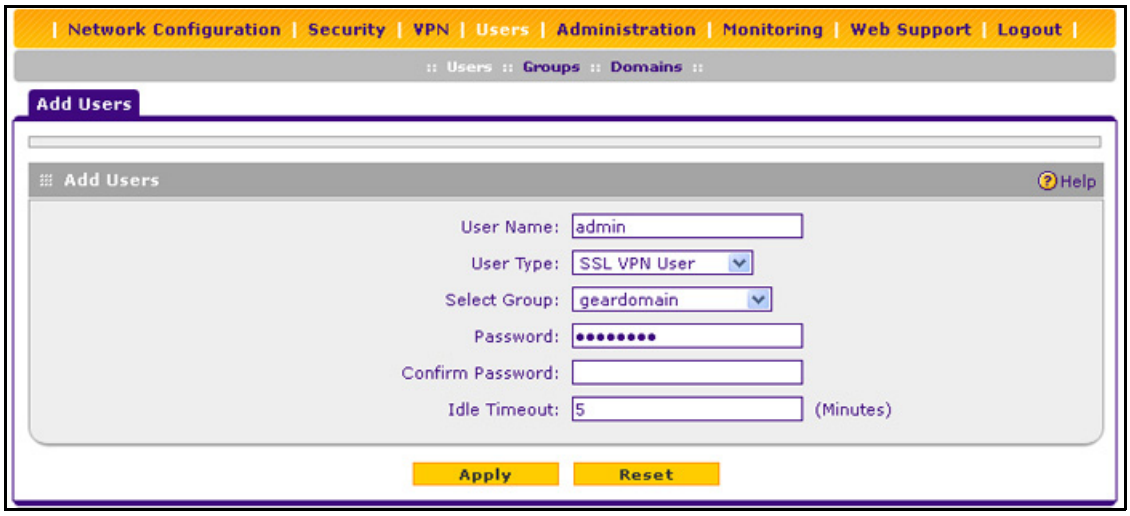


Figure 150.

3. Enter the settings as explained in the following table:

Table 65. Add Users screen settings

Setting	Description
User Name	A descriptive (alphanumeric) name of the user for identification and management purposes.
User Type	From the drop-down list, select one of the predefined user types that determines the access credentials: • **Administrator**. User who has full access and the capacity to change the wireless VPN firewall configuration (that is, read/write access). • **SSL VPN User**. User who can log in only to the SSL VPN portal. • **Guest User**. User who can only view the wireless VPN firewall configuration (that is, read-only access). • **IPSEC VPN User**. A user who can make an IPSec VPN connection only through a NETGEAR ProSafe VPN Client, and only when the XAUTH feature is enabled (see *Configure Extended Authentication (XAUTH)* on page 194). • **L2TP User**. User who can connect over an L2TP connection to an L2TP client that is located behind the wireless VPN firewall.
Select Group	The drop-down list shows the groups that are listed on the Group screen. From the drop-down list, select the group to which the user is assigned. For information about how to configure groups, see *Configure Groups* on page 251. **Note:** The user is assigned to the domain that is associated with the selected group.
Password	The password that the user needs to enter to gain access to the wireless VPN firewall. The password needs to contain alphanumeric, hyphen (-), or underscore (_) characters.

Table 65. Add Users screen settings (continued)

Setting	Description
Confirm Password	This field needs to be identical to the password that you entered in the Password field.
Idle Timeout	The period after which an idle user is automatically logged out of the web management interface. The default idle time-out period is 5 minutes.

4. Click **Apply** to save your settings. The user is added to the List of Users table.

➢ **To delete one or more user accounts:**

1. In the List of Users table, select the check box to the left of each user account that you want to delete, or click the **Select All** table button to select all accounts. You cannot delete a default user account.
2. Click the **Delete** table button.

Note: You cannot delete the default admin or guest user.

Set User Login Policies

You can restrict the ability of defined users to log in to the wireless VPN firewall's web management interface. You can also require or prohibit logging in from certain IP addresses or from particular browsers.

Configure Login Policies

➢ **To configure user login policies:**

1. Select **Users > Users**. The Users screen displays (see *Figure 149* on page 255).
2. In the Action column of the List of Users table, click the **Policies** table button for the user for which you want to set login policies. The policies submenu tabs display, with the Login Policies screen in view:

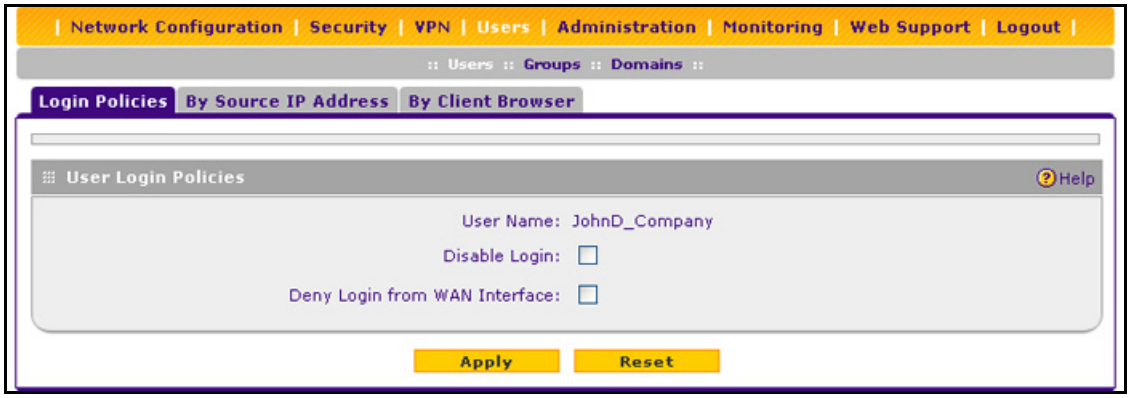


Figure 151.

3. Make the following optional selections:
   - To prohibit the user from logging in to the wireless VPN firewall, select the **Disable Login** check box.
   - To prohibit the user from logging in from the WAN interface, select the **Deny Login from WAN Interface** check box. In this case, the user can log in only from the LAN interface.

Note: For security reasons, the Deny Login from WAN Interface check box is selected by default for guests and administrators. The Disable Login check box is disabled (masked out) for administrators.

4. Click **Apply** to save your settings.

Configure Login Restrictions Based on IP Address

➢ **To restrict logging in based on IP address:**

1. Select **Users > Users**. The Users screen displays (see *Figure 149* on page 255).
2. In the Action column of the List of Users table, click the **Policies** table button for the user for which you want to set login policies. The policies submenu tabs display, with the Login Policies screen in view.
3. Click the **By Source IP Address** submenu tab. The By Source IP Address screen displays. (The following figure shows an IP address in the Defined Addresses table as an example.)

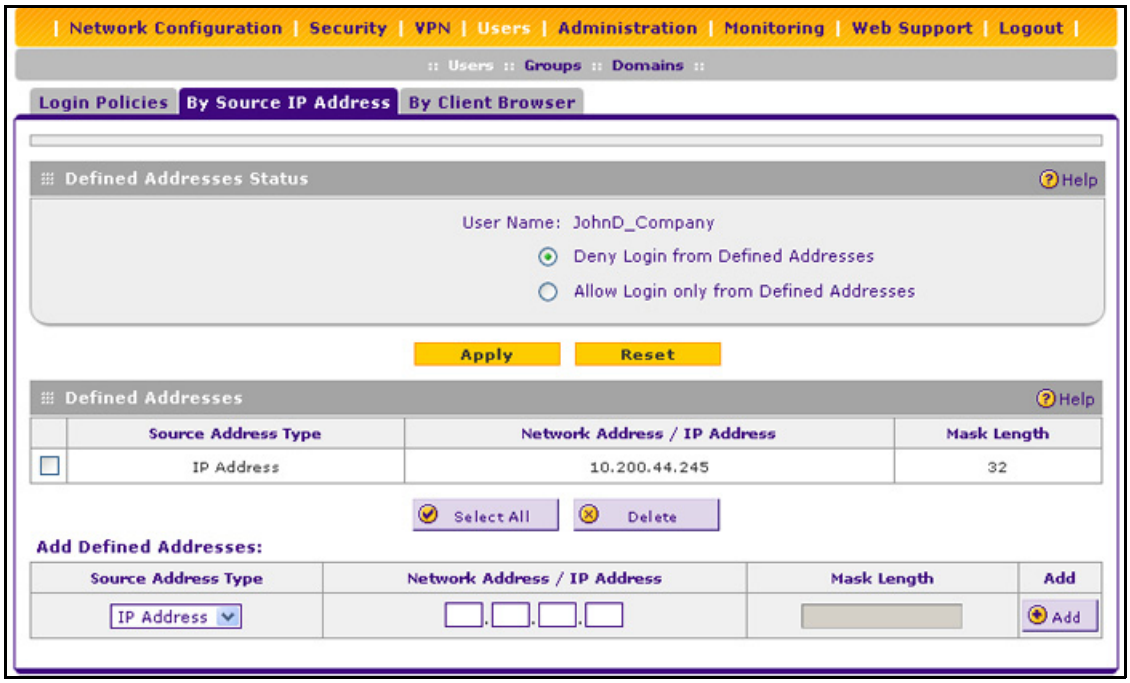


Figure 152.

4. In the Defined Addresses Status section of the screen, select one of the following radio buttons:
   - **Deny Login from Defined Addresses**. Deny logging in from the IP addresses in the Defined Addresses table.
   - **Allow Login only from Defined Addresses**. Allow logging in from the IP addresses in the Defined Addresses table.
5. Click **Apply** to save your settings.
6. In the Add Defined Addresses section of the screen, add an address to the Defined Addresses table by entering the settings as explained in the following table:

Table 66. Defined addresses settings

Setting	Description
Source Address Type	Select the type of address from the drop-down list: • **IP Address**. A single IP address. • **IP Network**. A subnet of IP addresses. You need to enter a netmask length in the Mask Length field.
Network Address / IP Address	Depending on your selection from the Source Address Type drop-down list, enter the IP address or the network address.
Mask Length	For a network address, enter the netmask length (0–32). **Note:** By default, a single IP address is assigned a netmask length of 32.

7. Click the **Add** table button. The address is added to the Defined Addresses table.
8. Repeat *step 6* and *step 7* for any other addresses that you want to add to the Defined Addresses table.

➢ **To delete one or more addresses:**

1. In the Defined Addresses table, select the check box to the left of each address that you want to delete, or click the **Select All** table button to select all addresses.
2. Click the **Delete** table button.

Configure Login Restrictions Based on Web Browser

➢ **To restrict logging in based on the user's browser:**

1. Select **Users > Users**. The Users screen displays (see *Figure 149* on page 255).
2. In the Action column of the List of Users table, click the **Policies** table button for the user for which you want to set login policies. The policies submenu tabs display, with the Login Policies screen in view.
3. Click the **By Client Browser** submenu tab. The By Client Browser screen displays. (The following figure shows a browser in the Defined Browsers table as an example.)

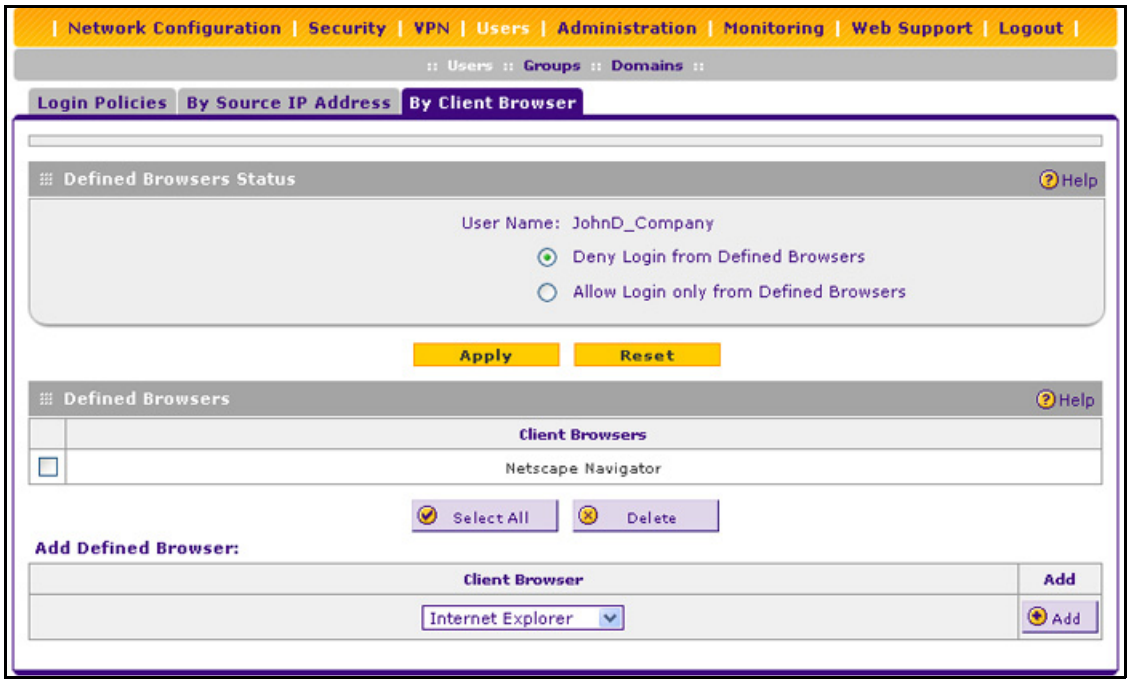


Figure 153.

4. In the Defined Browsers Status section of the screen, select one of the following radio buttons:
   - **Deny Login from Defined Browsers**. Deny logging in from the browsers in the Defined Browsers table.
   - **Allow Login only from Defined Browsers**. Allow logging in from the browsers in the Defined Browsers table.
5. Click **Apply** to save your settings.
6. In the Add Defined Browser section of the screen, add a browser to the Defined Browsers table by selecting one of the following browsers from the drop-down list:
   - **Internet Explorer**.
   - **Opera**.
   - **Netscape Navigator**.
   - **Firefox**. Mozilla Firefox.
   - **Mozilla**. Other Mozilla browsers.
7. Click the **Add** table button. The browser is added to the Defined Browsers table.
8. Repeat *step 6* and *step 7* for any other browsers that you want to add to the Defined Browsers table.

➢ **To delete one or more browsers:**

1. In the Defined Browsers table, select the check box to the left of each browser that you want to delete, or click the **Select All** table button to select all browsers.
2. Click the **Delete** table button.

Change Passwords and Other User Settings

For any user, you can change the password, user type, and idle time-out settings. Only administrators have read/write access. All other users have read-only access.

Note: The default administrator and default guest passwords for the web management interface are both **password**. NETGEAR recommends that you change the password for the administrator account to a more secure password, and that you configure a separate secure password for the guest account.

Note: The ideal password should contain no dictionary words from any language, and should be a mixture of letters (both uppercase and lowercase), numbers, and symbols. Your password can be up to 30 characters.

Note: After a factory defaults reset, the password and time-out value are changed back to **password** and 5 minutes, respectively.

➢ **To modify user settings, including passwords:**

1. Select **Users > Users**. The Users screen displays (see *Figure 149* on page 255).
2. In the Action column of the List of Users table, click the **Edit** table button for the user for which you want to modify the settings. The Edit Users screen displays:

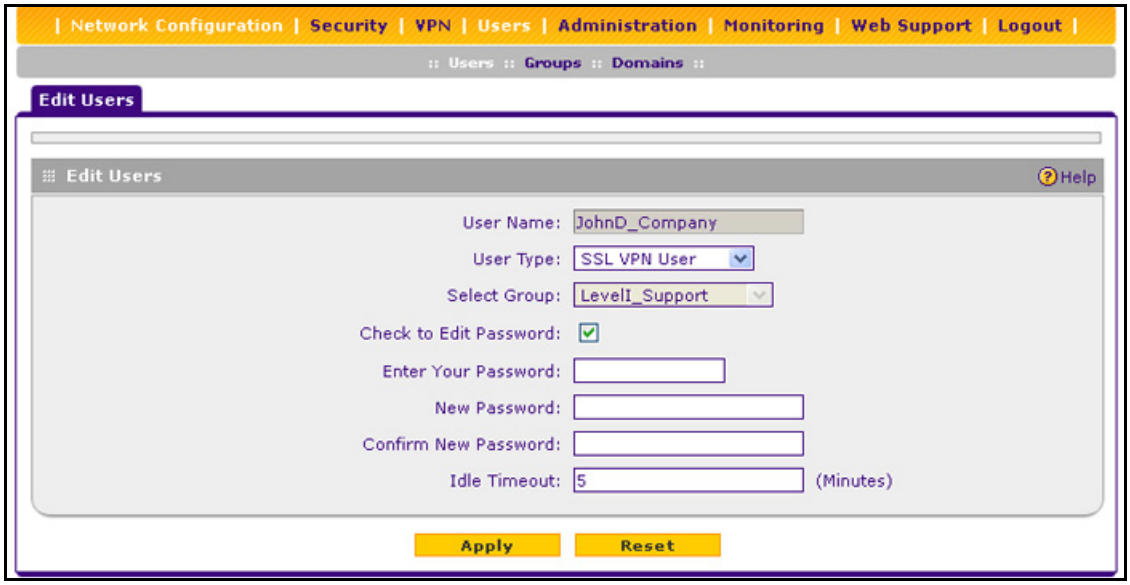


Figure 154.

3. Change the settings as explained in the following table:

Table 67. Edit User screen settings

Setting	Description	
Select User Type	From the drop-down list, select one of the predefined user types that determines the access credentials: • **SSL VPN User**. User who can log in only to the SSL VPN portal. • **Administrator**. User who has full access and the capacity to change the wireless VPN firewall configuration (that is, read/write access). • **Guest (readonly)**. User who can only view the wireless VPN firewall configuration (that is, read-only access). • **IPSEC VPN User**. A user who can make an IPSec VPN connection only through a NETGEAR ProSafe VPN Client, and only when the XAUTH feature is enabled (see *Configure Extended Authentication (XAUTH)* on page 194). • **L2TP User**. User who can connect over an L2TP connection to an L2TP client that is located behind the wireless VPN firewall.	
Check to Edit Password	Select this check box to make the password fields accessible to modify the password.	
	Enter Your Password	Enter the password with which you have logged in.
	New Password	Enter the new password.
	Confirm New Password	Reenter the new password for confirmation.
Idle Timeout	The period after which an idle user is automatically logged out of the web management interface. The default idle time-out period is 5 minutes.	

4. Click **Apply** to save your settings.

Manage Digital Certificates for VPN Connections

The wireless VPN firewall uses digital certificates (also known as X509 certificates) during the Internet Key Exchange (IKE) authentication phase to authenticate connecting IPSec VPN gateways or clients, or to be authenticated by remote entities. The same digital certificates are extended for secure web access connections over HTTPS (that is, SSL connections).

Digital certificates either can be self-signed or can be issued by certification authorities (CAs) such as an internal Windows server or an external organization such as Verisign or Thawte.

However, if the digital certificate contains the extKeyUsage extension, the certificate needs to be used for one of the purposes defined by the extension. For example, if the digital certificate contains the extKeyUsage extension that is defined for SNMPv2, the same certificate cannot be used for secure web management. The extKeyUsage would govern the certificate acceptance criteria on the wireless VPN firewall when the same digital certificate is being used for secure web management.

On the wireless VPN firewall, the uploaded digital certificate is checked for validity and purpose. The digital certificate is accepted when it passes the validity test and the purpose matches its use. The check for the purpose needs to correspond to its use for IPSec VPN, SSL VPN, or both. If the defined purpose is for IPSec VPN and SSL VPN, the digital

certificate is uploaded to both the IPSec VPN certificate repository and the SSL VPN certificate repository. However, if the defined purpose is for IPSec VPN only, the certificate is uploaded only to the IPSec VPN certificate repository.

The wireless VPN firewall uses digital certificates to authenticate connecting VPN gateways or clients, and to be authenticated by remote entities. A digital certificate that authenticates a server, for example, is a file that contains the following elements:

- A public encryption key to be used by clients for encrypting messages to the server.
- Information identifying the operator of the server.
- A digital signature confirming the identity of the operator of the server. Ideally, the signature is from a trusted third party whose identity can be verified.

You can obtain a digital certificate from a well-known commercial certification authority (CA) such as Verisign or Thawte, or you can generate and sign your own digital certificate. Because a commercial CA takes steps to verify the identity of an applicant, a digital certificate from a commercial CA provides a strong assurance of the server's identity. A self-signed digital certificate triggers a warning from most browsers because it provides no protection against identity theft of the server.

The wireless VPN firewall contains a self-signed digital certificate from NETGEAR. This certificate can be downloaded from the wireless VPN firewall login screen for browser import. However, NETGEAR recommends that you replace this digital certificate with a digital certificate from a well-known commercial CA prior to deploying the wireless VPN firewall in your network.

VPN Certificates Screen

To display the Certificates screen, select **VPN > Certificates**. Because of the large size of this screen, and because of the way the information is presented, the Certificates screen is divided and presented in this manual in three figures (*Figure 155* on page 264, *Figure 157* on page 266, and *Figure 159* on page 269).

The Certificates screen lets you to view the currently loaded digital certificates, upload a new digital certificate, and generate a certificate signing request (CSR). The wireless VPN firewall typically holds two types of digital certificates:

- CA certificates. Each CA issues its own digital certificate to validate communication with the CA and to verify the validity of digital certificates that are signed by the CA.
- Self-signed certificates. The digital certificates that are issued to you by a CA to identify your device.

The Certificates screen contains four tables that are explained in detail in the following sections:

- **Trusted Certificates (CA Certificate) table**. Contains the trusted digital certificates that were issued by CAs and that you uploaded (see *Manage VPN CA Certificates* on this page).
- **Active Self Certificates table**. Contains the self-signed certificates that were issued by CAs and that you uploaded (see *Manage VPN Self-Signed Certificates* on page 265).

- **Self Certificate Requests table**. Contains the self-signed certificate requests that you generated. These requests might or might not have been submitted to CAs, and CAs might or might not have issued digital certificates for these requests. Only the self-signed certificates in the Active Self Certificates table are active on the wireless VPN firewall (see *Manage VPN Self-Signed Certificates* on page 265).
- **Certificate Revocation Lists (CRL) table**. Contains the lists with digital certificates that have been revoked and are no longer valid, that were issued by CAs, and that you uploaded. Note, however, that the table displays only the active CAs and their critical release dates. (see *Manage the VPN Certificate Revocation List* on page 269).

Manage VPN CA Certificates

➢ **To view and upload trusted certificates:**

Select **VPN > Certificates**. The Certificates screen displays. (The following figure shows the top section of the screen with the trusted certificate information and an example certificate in the Trusted Certificates [CA Certificate] table.)

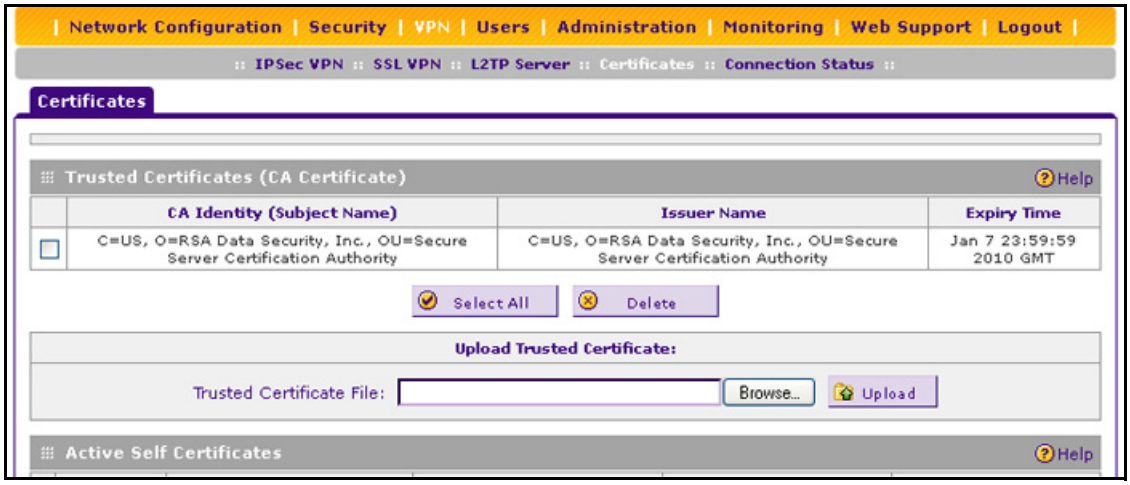

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
:: IPSec VPN :: SSL VPN :: L2TP Server :: Certificates :: Connection Status ::
Certificates
Trusted Certificates (CA Certificate)
Help
CA Identity (Subject Name)
Issuer Name
Expiry Time
C=US, O=RSA Data Security, Inc., OU=Secure Server Certification Authority
C=US, O=RSA Data Security, Inc., OU=Secure Server Certification Authority
Jan 7 23:59:59 2010 GMT
Select All
Delete
Upload Trusted Certificate:
Trusted Certificate File:
Browse...
Upload
Active Self Certificates
Help

Figure 155. Certificates, screen 1 of 3

The Trusted Certificates (CA Certificate) table lists the digital certificates of CAs and contains the following fields:

- **CA Identity (Subject Name)**. The organization or person to whom the digital certificate is issued.
- **Issuer Name**. The name of the CA that issued the digital certificate.
- **Expiry Time**. The date after which the digital certificate becomes invalid.

➢ **To upload a digital certificate of a trusted CA on the wireless VPN firewall:**

1. Download a digital certificate file from a trusted CA and store it on your computer.
2. In the Upload Trusted Certificates section of the screen, click the **Browse** button and navigate to the trusted digital certificate file that you downloaded on your computer.

3. Click the **Upload** table button. If the verification process on the wireless VPN firewall approves the digital certificate for validity and purpose, the digital certificate is added to the Trusted Certificates (CA Certificates) table.

➢ **To delete one or more digital certificates:**

1. In the Trusted Certificates (CA Certificate) table, select the check box to the left of each digital certificate that you want to delete, or click the **Select All** table button to select all digital certificates.
2. Click the **Delete** table button.

Manage VPN Self-Signed Certificates

Instead of obtaining a digital certificate from a CA, you can generate and sign your own digital certificate. However, a self-signed digital certificate triggers a warning from most browsers because it provides no protection against identity theft of the server. (The following figure shows an image of a browser security alert.)

There can be three reasons why a security alert is generated for a security certificate:

- The security certificate was issued by a company you have not chosen to trust.
- The date of the security certificate is invalid.
- The name on the security certificate is invalid or does not match the name of the site.

When a security alert is generated, the user can decide whether or not to trust the host.

Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The name on the security certificate is invalid or does not match the name of the site
Do you want to proceed?
Yes
No
View Certificate

Figure 156.

Generate a CSR and Obtain a Self-Signed Certificate from a CA

To use a self-signed certificate, you first need to request the digital certificate from a CA, and then download and activate the digital certificate on the wireless VPN firewall. To request a self-signed certificate from a CA, you need to generate a certificate signing request (CSR) for and on the wireless VPN firewall. The CSR is a file that contains information about your company and about the device that holds the certificate. Refer to the CA for guidelines about the information that you need to include in your CSR.

➢ **To generate a new CSR file, obtain a digital certificate from a CA, and upload it to the wireless VPN firewall:**

1. Select **VPN > Certificates**. The Certificates screen displays. The following figure shows the middle section of the screen with the Active Self Certificates section, Generate Self Certificate Request section, and Self Certificate Requests section. (The Self Certificate Requests table contains an example certificate.)

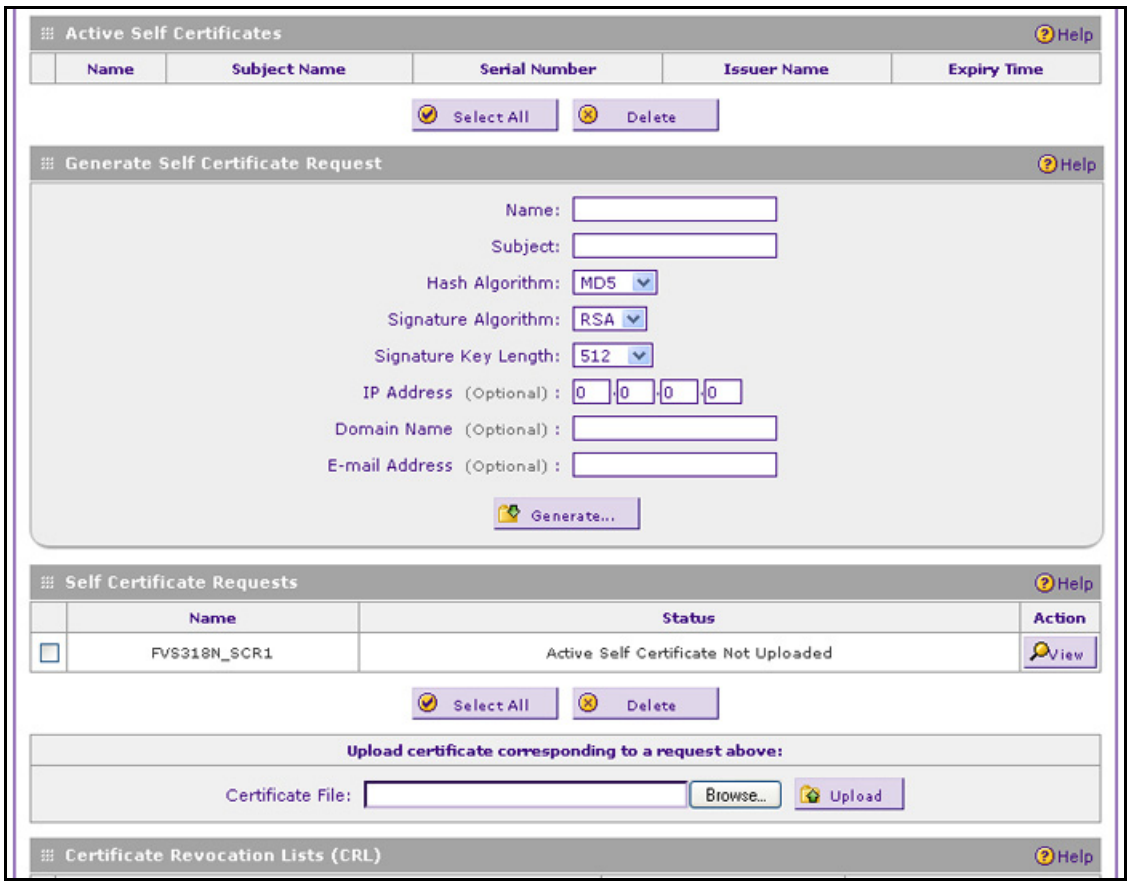


Figure 157. Certificates, screen 2 of 3

2. In the Generate Self Certificate Request section of the screen, enter the settings as explained in the following table:

Table 68. Generate self-signed certificate request settings

Setting	Description
Name	A descriptive name of the domain for identification and management purposes.
Subject	The name that other organizations see as the holder (owner) of the certificate. In general, use your registered business name or official company name for this purpose. **Note:** Generally, all of your certificates should have the same value in the Subject field.

Table 68. Generate self-signed certificate request settings (continued)

Setting	Description	
Hash Algorithm	From the drop-down list, select one of the following hash algorithms: • **MD5**. A 128-bit (16-byte) message digest, slightly faster than SHA-1. • **SHA-1**. A 160-bit (20-byte) message digest, slightly stronger than MD5.	
Signature Algorithm	Although this seems to be a drop-down list, the only possible selection is RSA. In other words, RSA is the default to generate a CSR.	
Signature Key Length	From the drop-down list, select one of the following signature key lengths in bits: • **512** • **1024** • **2048** **Note:** Larger key sizes might improve security, but might also decrease performance.	
Optional Fields	IP Address	Enter your fixed (static) IP address. If your IP address is dynamic, leave this field blank.
	Domain Name	Enter your Internet domain name, or leave this field blank.
	E-mail Address	Enter the email address of a technical contact in your company.

3. Click the **Generate** table button. A new SCR is created and added to the Self Certificate Requests table.
4. In the Self Certificate Requests table, click the **View** table button in the Action column to view the new SCR. The Certificate Request Data screen displays:

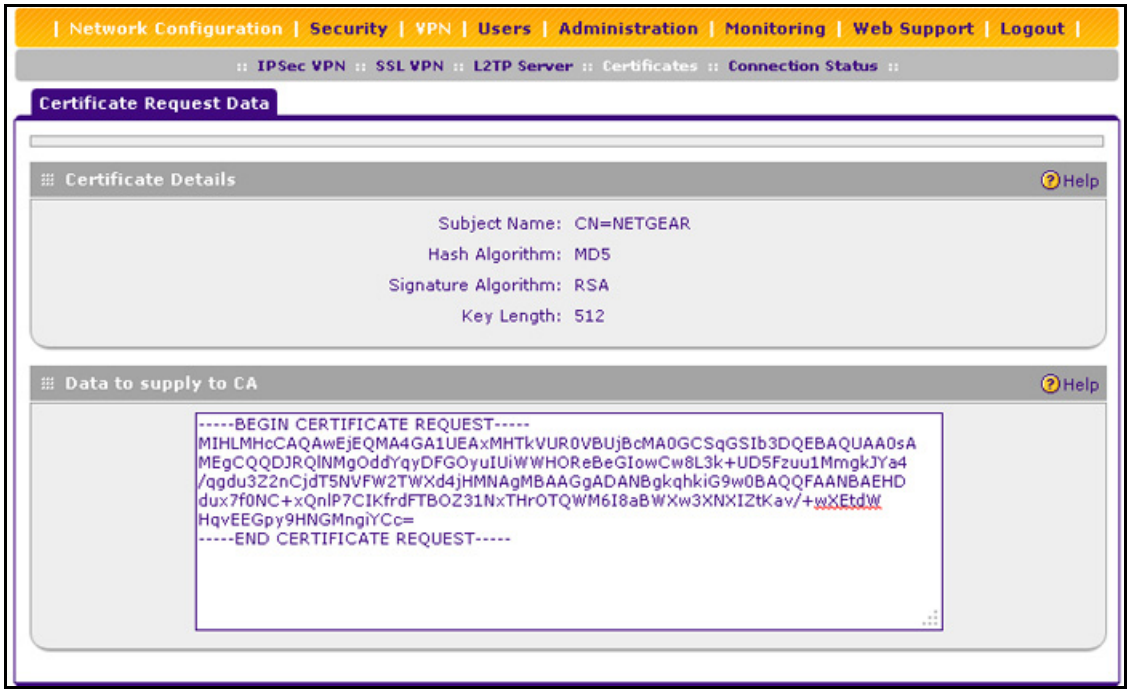


Figure 158.

5. Copy the contents of the Data to supply to CA text field into a text file, including all of the data contained from "-----BEGIN CERTIFICATE REQUEST-----" to "-----END CERTIFICATE REQUEST-----."
6. Submit your SCR to a CA:
   a. Connect to the website of the CA.
   b. Start the SCR procedure.
   c. When prompted for the requested data, copy the data from your saved text file (including "-----BEGIN CERTIFICATE REQUEST-----" and "-----END CERTIFICATE REQUEST-----").
   d. Submit the CA form. If no problems ensue, the digital certificate is issued by the CA.
7. Download the digital certificate file from the CA, and store it on your computer.
8. Return to the Certificates screen (see *Figure 157* on page 266) and locate the Self Certificate Requests section.
9. Select the check box next to the self-signed certificate request.
10. Click the **Browse** button and navigate to the digital certificate file from the CA that you just stored on your computer.
11. Click the **Upload** table button. If the verification process on the wireless VPN firewall approves the digital certificate for validity and purpose, the digital certificate is added to the Active Self Certificates table.

➢ **To delete one or more SCRs:**

1. In the Self Certificate Requests table, select the check box to the left of each SCR that you want to delete, or click the **Select All** table button to select all SCRs.
2. Click the **Delete** table button.

View and Manage Self-Signed Certificates

The Active Self Certificates table on the Certificates screen (see *Figure 157* on page 266) shows the digital certificates issued to you by a CA and available for use. For each self-signed certificate, the table lists the following information:

- **Name**. The name that you used to identify this digital certificate.
- **Subject Name**. The name that you used for your company and that other organizations see as the holder (owner) of the certificate.
- **Serial Number**. This is a serial number maintained by the CA. It is used to identify the digital certificate with the CA.
- **Issuer Name**. The name of the CA that issued the digital certificate.
- **Expiry Time**. The date on which the digital certificate expires. You should renew the digital certificate before it expires.

➢ **To delete one or more self-signed certificates:**

1. In the Active Self Certificates table, select the check box to the left of each self-signed certificate that you want to delete, or click the **Select All** table button to select all self-signed certificates.
2. Click the **Delete** table button.

Manage the VPN Certificate Revocation List

A Certificate Revocation List (CRL) file shows digital certificates that have been revoked and are no longer valid. Each CA issues its own CRLs. It is important that you keep your CRLs up-to-date. You should obtain the CRL for each CA regularly.

➢ **To view the currently loaded CRLs and upload a new CRL:**

1. Select **VPN > Certificates**. The Certificates screen displays. The following figure shows the bottom section of the screen with the Certificate Revocation Lists (CRL) table. (There is one example certificate in the table.)

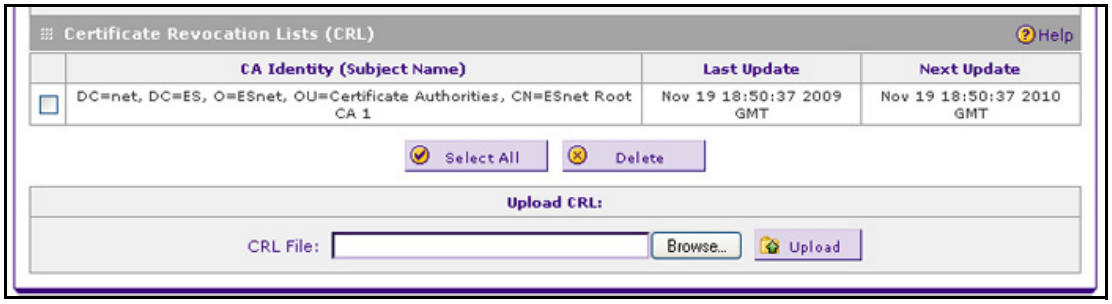


Figure 159. Certificates, screen 3 of 3

The Certificate Revocation Lists (CRL) table lists the active CAs and their critical release dates:

- **CA Identity**. The official name of the CA that issued the CRL.
- **Last Update**. The date when the CRL was released.
- **Next Update**. The date when the next CRL will be released.

2. In the Upload CRL section, click the **Browse** button and navigate to the CLR file that you previously downloaded from a CA.
3. Click the **Upload** table button. If the verification process on the wireless VPN firewall approves the CRL, the CRL is added to the Certificate Revocation Lists (CRL) table.

Note: If the table already contains a CRL from the same CA, the old CRL is deleted when you upload the new CRL.

➢ **To delete one or more CRLs:**

1. In the Certificate Revocation Lists (CRL) table, select the check box to the left of each CRL that you want to delete, or click the **Select All** table button to select all CRLs.
2. Click the **Delete** table button.

Network and System Management

9

This chapter describes the tools for managing the network traffic to optimize its performance and the system management features of the wireless VPN firewall. This chapter contains the following sections:

- *Performance Management*
- *System Management*

Performance Management

Performance management consists of controlling the traffic through the wireless VPN firewall so that the necessary traffic gets through when there is a bottleneck. You can either reduce unnecessary traffic or reschedule some traffic to low-peak times to prevent bottlenecks from occurring in the first place. The wireless VPN firewall has the necessary features and tools to help the network manager accomplish these goals.

Bandwidth Capacity

The maximum bandwidth capacity of the wireless VPN firewall in each direction is as follows:

- LAN side. 8000 Mbps (eight LAN ports at 1000 Mbps each).
- WAN side. 1000 Mbps (one active WAN port at 1000 Mbps).

In practice, the WAN-side bandwidth capacity is much lower when DSL or cable modems are used to connect to the Internet: The typical traffic rate is 1.5 Mbps. As a result, and depending on the traffic that is being carried, the WAN side of the wireless VPN firewall is the limiting factor for the data rate for most installations.

Features That Reduce Traffic

You can adjust the following features of the wireless VPN firewall in such a way that the traffic load on the WAN side decreases:

- LAN WAN outbound rules (also referred to as service blocking)
- DMZ WAN outbound rules (also referred to as service blocking)

- Content filtering
- Source MAC filtering

LAN WAN Outbound Rules and DMZ WAN Outbound Rules (Service Blocking)

You can control specific outbound traffic (from LAN to WAN and from the DMZ to WAN). The LAN WAN Rules screen and the DMZ WAN Rules screen list all existing rules for outbound traffic. If you have not defined any rules, only the default rule is listed. The default rule allows all outgoing traffic. Any outbound rule that you create restricts outgoing traffic and therefore decreases the traffic load on the WAN side.

WARNING!

This feature is for advanced administrators. Incorrect configuration might cause serious problems.

Each rule lets you specify the desired action for the connections that are covered by the rule:

- BLOCK always
- BLOCK by schedule, otherwise allow
- ALLOW always
- ALLOW by schedule, otherwise block

The following section summarizes the various criteria that you can apply to outbound rules in order to reduce traffic. For more information about outbound rules, see *Outbound Rules (Service Blocking)* on page 109. For detailed procedures on how to configure outbound rules, see *Set LAN WAN Rules* on page 116 and *Create DMZ WAN Rules* on page 119.

When you define outbound firewall rules, you can further refine their application according to the following criteria:

- **Services**. You can specify the services or applications, or groups of services or applications to be covered by an outbound rule. If the desired service or application does not display in the list, you need to define it using the Services screen (see *Service-Based Rules* on page 109 and *Add Customized Services* on page 136).
- **LAN users**. You can specify which computers on your network are affected by an outbound rule. There are several options:
  - **Any**. The rule applies to all PCs and devices on your LAN.
  - **Single address**. The rule applies to the address of a particular PC.
  - **Address range**. The rule applies to a range of addresses.
  - **Groups**. The rule applies to a group of PCs. (You can configure groups for LAN WAN outbound rules but not for DMZ WAN outbound rules.) The Known PCs and Devices table is an automatically maintained list of all known PCs and network devices and is generally referred to as the network database, which is described in *Manage the Network Database* on page 60. PCs and network devices are entered into the network database by various methods, which are described in *Manage IPv4 Groups and Hosts (IPv4 LAN Groups)* on page 59.

- **WAN users**. You can specify which Internet locations are covered by an outbound rule, based on their IP address:
  - **Any**. The rule applies to all Internet IP address.
  - **Single address**. The rule applies to a single Internet IP address.
  - **Address range**. The rule applies to a range of Internet IP addresses.
- **Schedule**. You can configure three different schedules to specify when a rule is applied. Once a schedule is configured, it affects all rules that use this schedule. You specify the days of the week and time of day for each schedule. For more information, see *Set a Schedule to Block or Allow Specific Traffic* on page 146.
- **QoS profile**. You can apply QoS profiles to outbound rules to regulate the priority of traffic. For information about QoS profiles, see *Preconfigured Quality of Service Profiles* on page 141.
- **Bandwidth profile**. You can define bandwidth profiles and then apply them to outbound rules to limit traffic. For information about how to define bandwidth profiles, see *Create Bandwidth Profiles* on page 139.

Content Filtering

If you want to reduce traffic by preventing access to certain sites on the Internet, you can use the wireless VPN firewall's content-filtering feature. By default, this feature is disabled; all requested traffic from any website is allowed with the exception of web content categories that are mentioned in *Configure Content Filtering* on page 142.

The wireless VPN firewall provides the following methods to filter web content in order to reduce traffic:

- **Keyword blocking**. You can specify words that, should they appear in the website name (URL) or newsgroup name, cause that site or newsgroup to be blocked by the wireless VPN firewall.
- **Web object blocking**. You can block the following web component types: embedded objects (ActiveX and Java), proxies, and cookies.

To further narrow down the content filtering, you can configure groups to which the content-filtering rules apply and trusted domains for which the content-filtering rules do not apply.

Source MAC Filtering

If you want to reduce outgoing traffic by preventing Internet access by certain PCs on the LAN, you can use the source MAC filtering feature to drop the traffic received from the PCs with the specified MAC addresses. By default, this feature is disabled; all traffic received from PCs with any MAC address is allowed. See *Enable Source MAC Filtering* on page 147 for the procedure on how to use this feature.

Features That Increase Traffic

The following features of the wireless VPN firewall tend to increase the traffic load on the WAN side:

- LAN WAN inbound rules (also referred to as port forwarding)
- DMZ WAN inbound rules (also referred to as port forwarding)
- Port triggering
- Enabling the DMZ port
- Configuring exposed hosts
- Configuring VPN tunnels

LAN WAN Inbound Rules and DMZ WAN Inbound Rules (Port Forwarding)

The LAN WAN Rules screen and the DMZ WAN Rules screen list all existing rules for inbound traffic (from WAN to LAN and from WAN to the DMZ). If you have not defined any rules, only the default rule is listed. The default rule blocks all access from outside except responses to requests from the LAN side. Any inbound rule that you create allows additional incoming traffic and therefore increases the traffic load on the WAN side.

WARNING!

This feature is for advanced administrators. Incorrect configuration might cause serious problems.

Each rule lets you specify the desired action for the connections covered by the rule:

- BLOCK always
- BLOCK by schedule, otherwise allow
- ALLOW always
- ALLOW by schedule, otherwise block

The following section summarizes the various criteria that you can apply to inbound rules and that might increase traffic. For more information about inbound rules, see *Inbound Rules (Port Forwarding)* on page 112. For detailed procedures on how to configure inbound rules, see *Set LAN WAN Rules* on page 116 and *Create DMZ WAN Rules* on page 119.

When you define inbound firewall rules, you can further refine their application according to the following criteria:

- **Services**. You can specify the services or applications, or groups of services or applications to be covered by an inbound rule. If the desired service or application does not display in the list, you need to define it using the Services screen (see *Service-Based Rules* on page 109 and *Add Customized Services* on page 136).
- **WAN destination IP address**. You can specify the destination IP address for incoming traffic. Traffic is directed to the specified address only when the destination IP address of the incoming packet matches the IP address of the selected WAN interface.

- **LAN users**. You can specify which computers on your network are affected by an inbound rule. There are several options:
  - **Any**. The rule applies to all PCs and devices on your LAN.
  - **Single address**. The rule applies to the address of a particular PC.
  - **Address range**. The rule applies to a range of addresses.
  - **Groups**. The rule is applied to a group of PCs. (You can configure groups for LAN WAN outbound rules but not for DMZ WAN outbound rules.) The Known PCs and Devices table is an automatically maintained list of all known PCs and network devices and is generally referred to as the network database, which is described in *Manage the Network Database* on page 60. PCs and network devices are entered into the network database by various methods, which are described in *Manage IPv4 Groups and Hosts (IPv4 LAN Groups)* on page 59.
- **WAN users**. You can specify which Internet locations are covered by an inbound rule, based on their IP address:
  - **Any**. The rule applies to all Internet IP address.
  - **Single address**. The rule applies to a single Internet IP address.
  - **Address range**. The rule applies to a range of Internet IP addresses.
- **Schedule**. You can configure three different schedules to specify when a rule is applied. Once a schedule is configured, it affects all rules that use this schedule. You specify the days of the week and time of day for each schedule. For more information, see *Set a Schedule to Block or Allow Specific Traffic* on page 146.
- **QoS profile**. You can apply QoS profiles to inbound rules to regulate the priority of traffic. For information about QoS profiles, see *Preconfigured Quality of Service Profiles* on page 141.
- **Bandwidth profile**. You can define bandwidth profiles and then apply them to inbound rules to limit traffic. For information about how to define bandwidth profiles, see *Create Bandwidth Profiles* on page 139.

Port Triggering

Port triggering allows some applications running on a LAN network to be available to external applications that would otherwise be partially blocked by the firewall. Using the port-triggering feature requires that you know the port numbers used by the application. Without port triggering, the response from the external application would be treated as a new connection request rather than a response to a request from the LAN network. As such, it would be handled in accordance with the inbound port-forwarding rules, and most likely would be blocked.

For the procedure on how to configure port triggering, see *Configure Port Triggering* on page 151.

DMZ Port

The demilitarized zone (DMZ) is a network that, by default, has fewer firewall restrictions when compared to the LAN. The DMZ can be used to host servers (such as a web server,

FTP server, or email server) and provide public access to them. The eighth LAN port on the wireless VPN firewall (the rightmost LAN port) can be dedicated as a hardware DMZ port to safely provide services to the Internet without compromising security on your LAN. By default, the DMZ port and both inbound and outbound DMZ traffic are disabled. Enabling the DMZ port and allowing traffic to and from the DMZ increases the traffic through the WAN ports.

For information about how to enable the DMZ port, see *Configure and Enable the DMZ Port for IPv4 Traffic* on page 72. For the procedures about how to configure DMZ traffic rules, see *Create DMZ WAN Rules* on page 119.

Exposed Hosts

Specifying an exposed host allows you to set up a computer or server that is available to anyone on the Internet for services that you have not yet defined. For an example of how to set up an exposed host, see *LAN WAN or DMZ WAN Inbound Rule: Specifying an Exposed Host* on page 130.

VPN and L2TP Tunnels

The wireless VPN firewall supports site-to-site IPSec VPN tunnels, dedicated SSL VPN tunnels, and L2TP tunnels. Each tunnel requires extensive processing for encryption and authentication, thereby increasing traffic through the WAN ports.

For information about IPSec VPN tunnels, see *Chapter 6, Virtual Private Networking Using IPv4 IPSec and L2TP Connections*. For information about SSL VPN tunnels, see *Chapter 7, Virtual Private Networking Using IPv4 SSL Connections*.

Use QoS and Bandwidth Assignment to Shift the Traffic Mix

By specifying QoS and bandwidth profiles and assigning these profiles to outbound and inbound firewall rules, you can shift the traffic mix to aim for optimum performance of the wireless VPN firewall.

Assign QoS Profiles

The QoS profile settings determine the priority and, in turn, the quality of service for the traffic passing through the wireless VPN firewall. You can assign a QoS profile to a firewall rule. The QoS is set individually for each service. You can change the mix of traffic through the WAN ports by granting some services a higher priority than others:

- You can accept the default priority defined by the service itself by not changing its QoS setting.
- You can change the priority to a higher or lower value than its default setting to give the service higher or lower priority than it otherwise would have.

For more information about QoS profiles, see *Preconfigured Quality of Service Profiles* on page 141.

Assign Bandwidth Profiles

When you apply a QoS profile, the WAN bandwidth does not change. You change the WAN bandwidth that is assigned to a service or application by applying a bandwidth profile. The purpose of bandwidth profiles is to provide a method for allocating and limiting traffic, thus allocating LAN users sufficient bandwidth while preventing them from consuming all the bandwidth on your WAN links.

For more information about bandwidth profiles, see *Create Bandwidth Profiles* on page 139.

Monitoring Tools for Traffic Management

The wireless VPN firewall includes several tools that can be used to monitor the traffic conditions of the firewall and content-filtering engine and to monitor the users' access to the Internet and the types of traffic that they are allowed to have. See *Chapter 10, Monitor System Access and Performance*, for a description of these tools.

System Management

System management tasks are described in the following sections:

- *Change Passwords and Administrator and Guest Settings*
- *Configure Remote Management Access*
- *Use a Simple Network Management Protocol Manager*
- *Manage the Configuration File*
- *Update the Firmware*
- *Configure Date and Time Service*

Change Passwords and Administrator and Guest Settings

The default administrator and default guest passwords for the web management interface are both password. NETGEAR recommends that you change the password for the administrator account to a more secure password, and that you configure a separate secure password for the guest account.

➢ **To modify the administrator and guest passwords and idle time-out settings:**

1. Select **Users > Users**. The Users screen displays. (The following figure shows the wireless VPN firewall's default users—admin and guest—and, as an example, several other users in the List of Users table.)

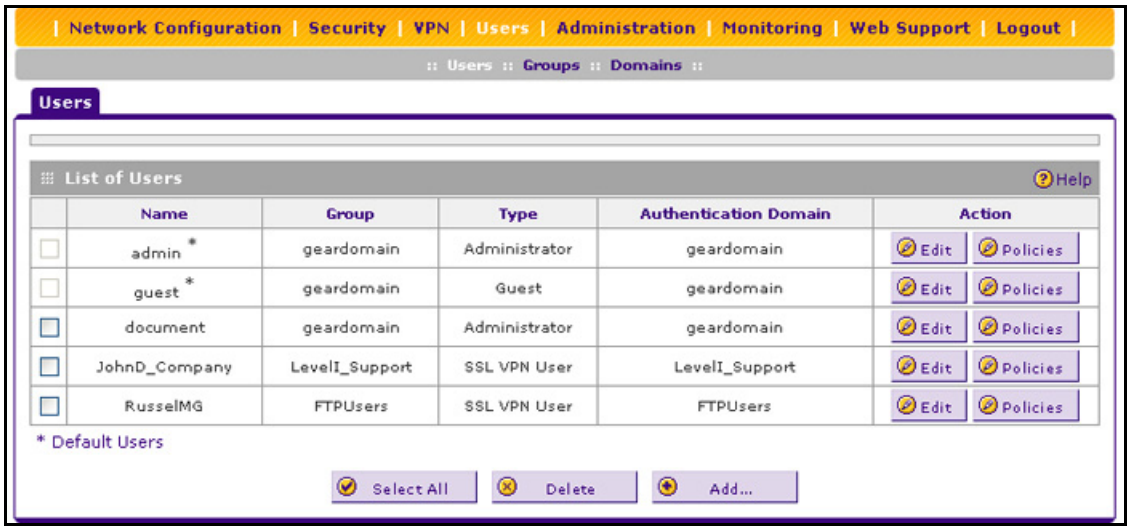


Figure 160.

2. In the Action column of the List of Users table, click the **Edit** table button for the user with the name admin. The Edit Users screen displays:

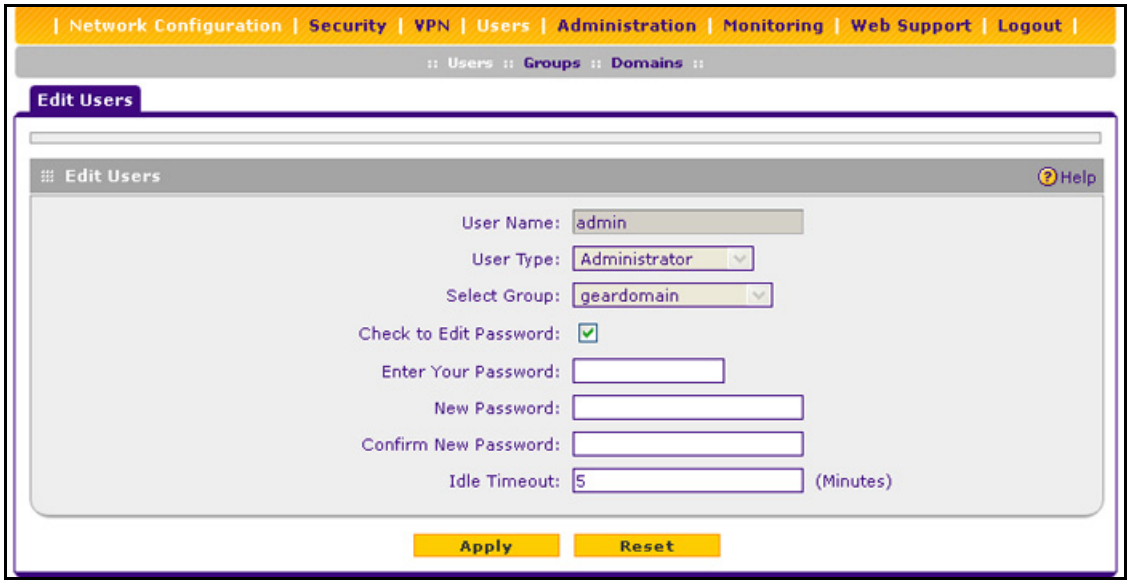


Figure 161.

You cannot modify the administrator user name, user type, or group assignment.

3. Select the **Check to Edit Password** check box. The password fields become available.
4. Enter the old password, enter the new password, and then confirm the new password.

Note: The ideal password should contain no dictionary words from any language, and should be a mixture of letters (both uppercase and lowercase), numbers, and symbols. Your password can be up to 30 characters.

5. As an option, you can change the idle time-out for an administrator login session. Enter a new number of minutes in the Idle Timeout field. (The default setting is 5 minutes.)
6. Click **Apply** to save your settings.
7. Repeat *step 1* through *step 6* for the user with the name guest.

Note: After a factory defaults reset, the password and time-out value are changed back to password and 5 minutes, respectively.

You can also change the administrator login policies:

- Disable login. Deny login access.

Note: You obviously do not want to deny login access to yourself if you are logged in as an administrator.

- Deny login access from a WAN interface. By default, the administrator can log in from a WAN interface.
- Deny or allow login access from specific IP addresses. By default, the administrator can log in from any IP address.

Note: For enhanced security, restrict access to as few external IP addresses as practical.

- Deny or allow login access from specific browsers. By default, the administrator can log in from any browser.

In general, these policy settings work well for an administrator. However, you can change the administrator login policies as explained in *Set User Login Policies* on page 257.

Configure Remote Management Access

An administrator can configure, upgrade, and check the status of the wireless VPN firewall over the Internet through a Secure Sockets Layer (SSL) VPN connection.

Note: When remote management is enabled and administrative access through a WAN interface is granted (see *Configure Login Policies* on page 257), the wireless VPN firewall's web management interface is accessible to anyone who knows its IP address and default password. Because a malicious WAN user can reconfigure the wireless VPN firewall and misuse it in many ways, NETGEAR highly recommends that you change the admin and guest default passwords before continuing (see *Change Passwords and Administrator and Guest Settings* on page 276).

➢ **To configure the wireless VPN firewall for remote management:**

1. Select **Administration > Remote Management**. The Remote Management screen displays:

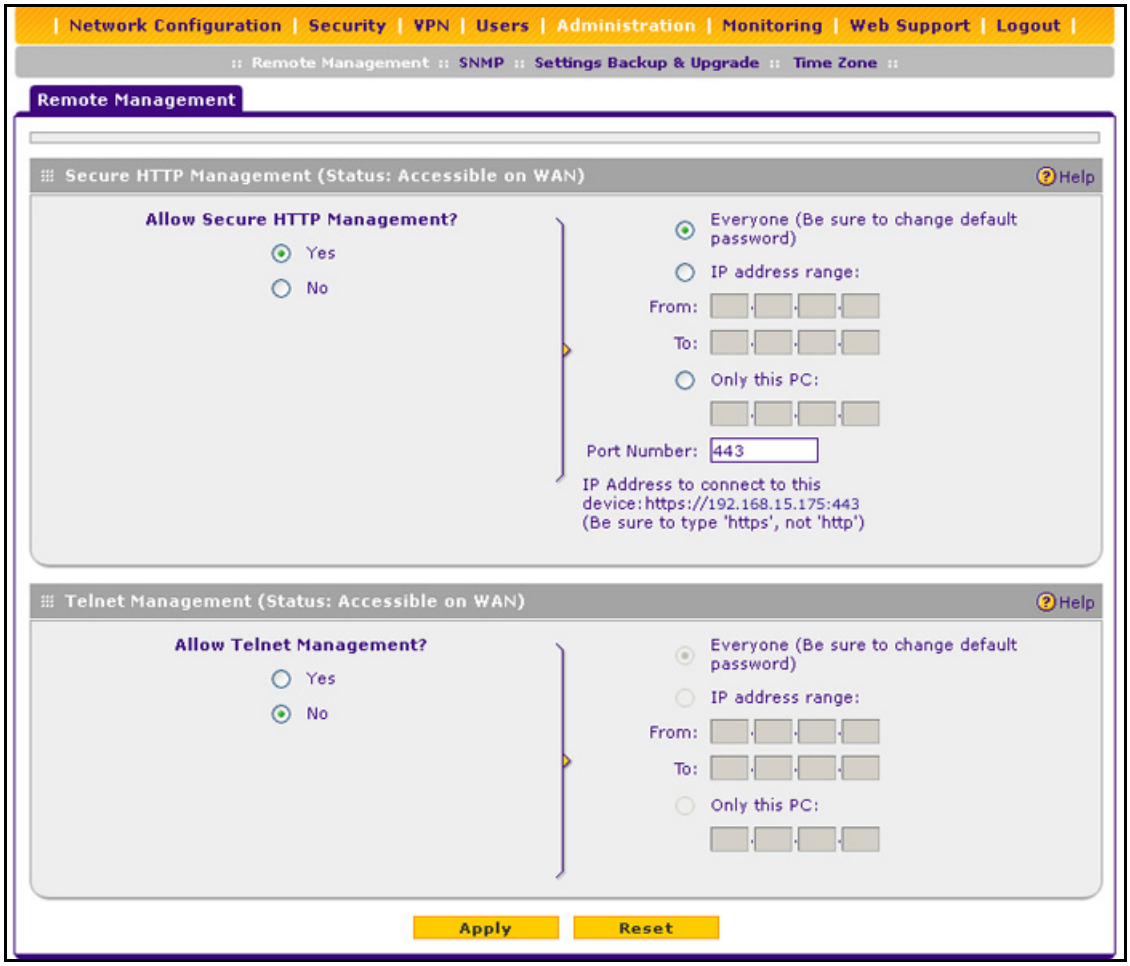


Figure 162.

2. Enter the settings as explained in the following table:

Table 69. Remote Management screen settings

Setting	Description
Secure HTTP Management	
Allow Secure HTTP Management?	To enable secure HTTP management, select the **Yes** radio button, which is the default setting. To disable secure HTTP management, select the **No** radio button.
	Specify the addresses through which access is allowed by selecting one of the following radio buttons: • **Everyone**. There are no IP address restrictions. • **IP address range**. Only users who use devices in the specified IP address range can securely manage over an HTTP connection. In the From fields, type the start IP address of the range; in the To fields, type the end IP address of the range. • **Only this PC**. Only a user who uses the device with the specified IP address can securely manage over an HTTP connection. Type the IP address in the fields.
Port Number	Enter the port number through which access is allowed. The default port number is 443. **Note:** The URL through which you can securely manage over an HTTP connection displays below the Port Number field.
Telnet Management	
Allow Telnet Management?	To enable Telnet management, select the **Yes** radio button. To disable Telnet management, select the **No** radio button, which is the default setting.
	Specify the addresses through which access is allowed by selecting one of the following radio buttons: • **Everyone**. There are no IP address restrictions. • **IP address range**. Only users who use devices in the specified IP address range can manage over a Telnet connection. In the From fields, type the start IP address of the range; in the To fields, type the end IP address of the range. • **Only this PC**. Only a user who uses the device with the specified IP address can manage over a Telnet connection. Type the IP address in the fields.

WARNING!

If you are remotely connected to the wireless VPN firewall and you select the No radio button to disable secure HTTP management, you and all other SSL VPN users are disconnected when you click Apply.

3. Click **Apply** to save your changes.

When remote management is enabled, you need to use an SSL connection to access the wireless VPN firewall from the Internet. You need to enter https:// (*not* http://) and type the wireless VPN firewall's WAN IP address and port number in your browser. For example, if

the wireless VPN firewall's WAN IP address is 192.168.15.175 and the port number is 443, type the following in your browser: **https://192.168.15.175:443**.

The wireless VPN firewall's remote login URL is:

https://<*IP_address*>:<*port_number*> or
https://<*FullyQualifiedDomainName*>:<*port_number*>

Note: For enhanced security, restrict access to as few external IP addresses as practical. See *Set User Login Policies* on page 257 for instructions on restricting administrator access by IP address.

Note: To maintain security, the wireless VPN firewall rejects a login that uses http://*address* rather than the SSL https://*address*.

Note: The first time that you remotely connect to the wireless VPN firewall with a browser through an SSL connection, you might get a warning message regarding the SSL certificate. If you are using a Windows computer with Internet Explorer 5.5 or later, simply click **Yes** to accept the certificate.

Tip: If you are using a Dynamic DNS service such as TZO, you can identify the WAN IP address of your wireless VPN firewall by running **`tracert`** from the Windows Run menu option. Trace the route to your registered FQDN. For example, enter **`tracert wireless VPN firewall.mynetgear.net`**, and the WAN IP address that your ISP assigned to the wireless VPN firewall is displayed.

Use a Simple Network Management Protocol Manager

Simple Network Management Protocol (SNMP) forms part of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). SNMP is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (and sometimes set) by managing applications.

SNMP lets you monitor and manage your wireless VPN firewall from an SNMP manager. It provides a remote means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

➢ **To configure the SNMP settings:**

1. Select **Administration > SNMP**. The SNMP screen displays. (The following figure contains an example.)

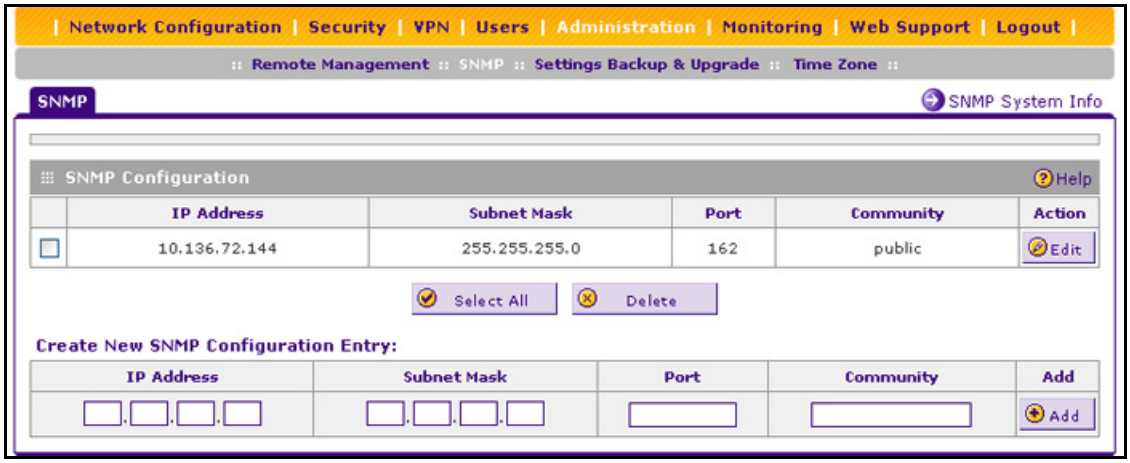


Figure 163.

The SNMP Configuration table shows the following columns:

- **IP Address**. The IP address of the SNMP manager.
- **Subnet Mask**. The subnet mask of the SNMP manager.
- **Port**. The trap port number of the SNMP manager.
- **Community**. The trap community string of the SNMP manager.

2. To specify a new SNMP configuration, in the Create New SNMP Configuration Entry section of the screen, enter the settings as explained in the following table:

Table 70. SNMP screen settings

Setting	Description
IP Address	Enter the IP address of the new SNMP manager.
Subnet Mask	Enter the subnet mask of the new SNMP manager. Note the following: • If you want to narrow down the number of devices that can access the wireless VPN firewall through the host IP address and receive traps, enter an IP address with a subnet mask of 255.255.255.252. • If you want to allow a subnet to access the wireless VPN firewall through the host IP address and receive traps, enter an IP address with a subnet mask of 255.0.0.0. The traps are received at the IP address, but almost the entire subnet has access through the community string.
Port	Enter the port number of the new SNMP manager. The default port number is 162.
Community	Enter the community string that allows the SNMP manager access to the MIB objects of the wireless VPN firewall for the purpose of reading only.

3. Click **Add** to add the new SNMP configuration to the SNMP Configuration table.

To edit an SNMP configuration:

1. On the SNMP screen (see the previous figure), click the **Edit** button in the Action column for the SNMP configuration that you want to modify. The Edit SNMP screen displays.

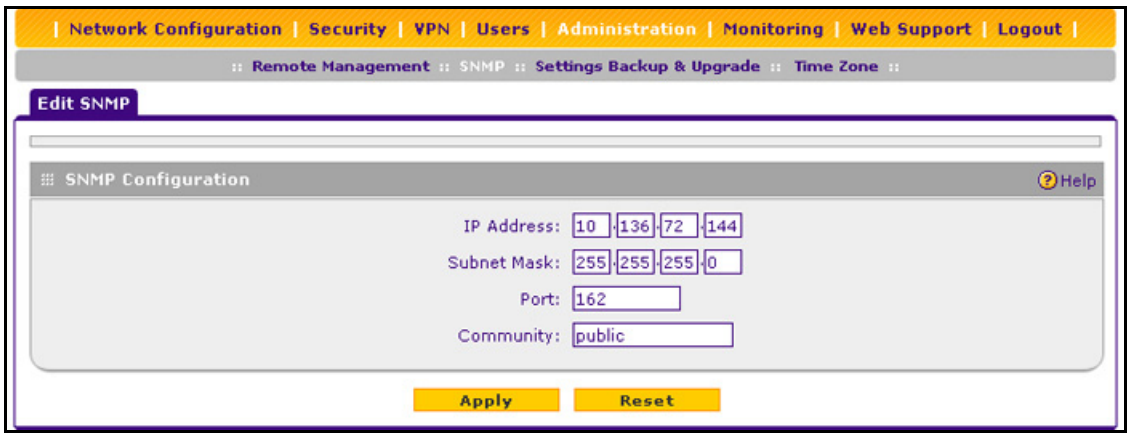

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
Remote Management :: SNMP :: Settings Backup & Upgrade :: Time Zone
Edit SNMP
SNMP Configuration
Help
IP Address: 10 136 72 144
Subnet Mask: 255 255 255 0
Port: 162
Community: public
Apply
Reset

Figure 164.

2. Modify the settings as explained in the previous table.
3. Click **Apply** to save your settings.

To delete one or more SNMP configurations:

1. On the SNMP screen (see *Figure 163* on page 282), select the check box to the left of each SNMP configuration that you want to delete, or click the **Select All** table button to select all SNMP configurations.
2. Click the **Delete** table button.

To configure the SNMP system information:

1. On the SNMP screen (see *Figure 163* on page 282), click the **SNMP System Info** option arrow in the upper right of the screen. The SNMP SysConfiguration screen displays.

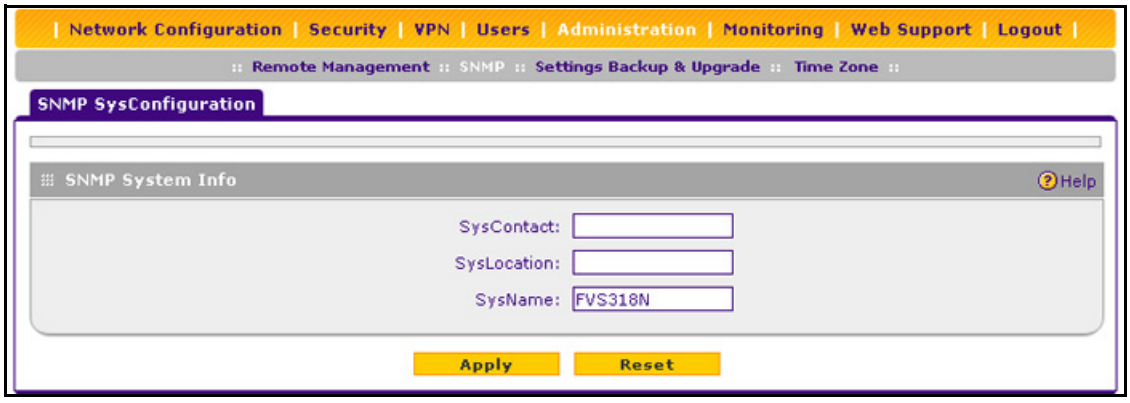

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
Remote Management :: SNMP :: Settings Backup & Upgrade :: Time Zone
SNMP SysConfiguration
SNMP System Info
Help
SysContact:
SysLocation:
SysName: FVS318N
Apply
Reset

Figure 165.

2. Enter the settings as explained in the following table:

Table 71. SNMP SysConfiguration screen settings

Setting	Description
SysContact	Enter the SNMP system contact information that is available to the SNMP manager. This setting is optional.
SysLocation	Enter the physical location of the wireless VPN firewall. This setting is optional.
SysName	Enter the name of the wireless VPN firewall for SNMP identification purposes. The default name is FVS318N.

3. Click **Apply** to save your changes.

Manage the Configuration File

The configuration settings of the wireless VPN firewall are stored in a configuration file on the wireless VPN firewall. This file can be saved (backed up) to a PC, retrieved (restored) from the PC, cleared to factory default settings, or upgraded to a new version.

Once the wireless VPN firewall is installed and works correctly, make a backup of the configuration file to a computer. If necessary, you can later restore the wireless VPN firewall settings from this file.

The Backup & Restore Settings screen lets you:

- Back up and save a copy of the current settings (see *Back Up Settings* on page 285)
- Restore saved settings from the backed-up file (see *Restore Settings* on page 286)
- Revert to the factory default settings (see *Revert to Factory Default Settings* on page 286)
- Update the firmware (see *Update the Firmware* on page 287)

To display the Settings Backup and Firmware Upgrade screen, select **Administration > Settings Backup & Upgrade**.

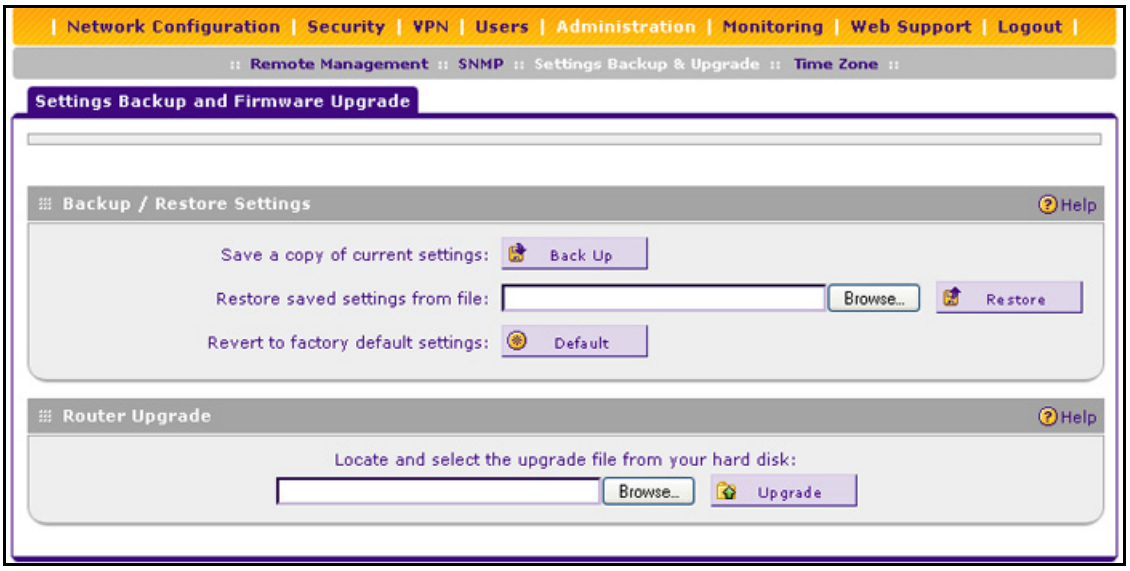

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
Remote Management :: SNMP :: Settings Backup & Upgrade :: Time Zone ::
Settings Backup and Firmware Upgrade
Backup / Restore Settings
Help
Save a copy of current settings:
Back Up
Restore saved settings from file:
Browse...
Restore
Revert to factory default settings:
Default
Router Upgrade
Help
Locate and select the upgrade file from your hard disk:
Browse...
Upgrade

Figure 166.

Back Up Settings

The backup feature saves all wireless VPN firewall settings to a file. Back up your settings periodically, and store the backup file in a safe place.

Tip: You can use a backup file to export all settings to another wireless VPN firewall that has the same language and management software versions. Remember to change the IP address of the second wireless VPN firewall before deploying it to eliminate IP address conflicts on the network.

➢ **To back up settings:**

1. On the Settings Backup and Firmware Upgrade screen (see the previous figure), next to Save a copy of current settings, click the **Backup** button to save a copy of your current settings. A screen displays, showing the file name of the backup file (FVS318N.cfg).
2. Select **Save file**, and then click **OK**.
3. Open the folder in which you have saved the backup file, and then verify that it has been saved successfully.

Note the following:

- If your browser is not configured to save downloaded files automatically, locate the folder in which you want to save the file, specify the file name, and save the file.
- If your browser is configured to save downloaded files automatically, the file is saved to your browser's download location on the hard disk.

Restore Settings

WARNING!

Restore only settings that were backed up from the same software version. Restoring settings from a different software version can corrupt your backup file or the wireless VPN firewall system software.

➢ **To restore settings from a backup file:**

1. On the Settings Backup and Firmware Upgrade screen (see the previous figure), next to Restore saved settings from file, click **Browse**.
2. Locate and select the previously saved backup file (by default, FVS318N.cfg).
3. After you have selected the file, click the **Restore** button. A warning message might display, and you might have to confirm that you want to restore the configuration.

The wireless VPN firewall reboots. During the reboot process, the Settings Backup and Firmware Upgrade screen might remain visible, or a status message with a counter might show the number of seconds left until the reboot process is complete. The reboot process takes about 160 seconds. (If you can see the unit: The reboot process is complete when the Test LED on the front panel goes off.)

WARNING!

Once you start restoring settings, do *not* interrupt the process. Do not try to go online, turn off the wireless VPN firewall, shut down the computer, or do anything else to the wireless VPN firewall until the settings have been fully restored.

Revert to Factory Default Settings

➢ **To reset the wireless VPN firewall to the original factory defaults settings:**

Use one of the following two methods:

- Using a sharp object, press and hold the factory default **Reset** button on the rear panel of the wireless VPN firewall (see *Rear Panel* on page 17) for about 8 seconds until the Test LED turns on and begins to blink (about 30 seconds). To restore the factory default settings when you do not know the administration password or IP address, you need to use the factory default Reset button method.
- On the Settings Backup and Firmware Upgrade screen (see the previous figure), next to Revert to factory defaults settings, click the **Default** button, and confirm your selection.

The wireless VPN firewall reboots. If you use the software Default button, the Settings Backup and Firmware Upgrade screen might remain visible during the reboot process, or a status message with a counter might show the number of seconds left until the reboot

process is complete. The reboot process takes about 160 seconds. (If you can see the unit: The reboot process is complete when the Test LED on the front panel goes off.)

WARNING!

When you press the hardware factory default Reset button or click the software Default button, the wireless VPN firewall settings are erased. All firewall rules, VPN policies, LAN and WAN settings, and other settings are lost. Back up your settings if you intend on using them.

Note: After you reboot with factory default settings, the wireless VPN firewall's password is **password**, and the LAN IP address is **192.168.1.1**.

Update the Firmware

You can install a different version of the wireless VPN firewall firmware from the Settings Backup and Firmware Upgrade screen. To view the current version of the firmware that the wireless VPN firewall is running, from the main menu, select **Monitoring**. The Router Status screen displays, showing the firmware version in the System Info section of the screen. After you have updated the firmware, the new firmware version is displayed.

➢ **To download a firmware version and upgrade the firmware:**

1. Go to the NETGEAR website at *http://support.netgear.com*.
2. Navigate to the FVS318N support page, and click the **Downloads** tab.
3. Click the desired firmware version to reach the download page. Be sure to read the release notes on the download page before upgrading the wireless VPN firewall's software.
4. On the Settings Backup and Firmware Upgrade screen of the wireless VPN firewall (see the previous figure), in the Router Upgrade section, click **Browse**.
5. Locate and select the downloaded firmware file.
6. Click **Upload**. The upgrade process starts.

   During the upgrade process, the Settings Backup and Firmware Upgrade screen remains visible and a status bar shows the progress of the upgrade process. The upgrade process can take up to 10 minutes. When the status bar shows that the upgrade process is complete, it can take another 10 minutes before the wireless VPN firewall reboots.

WARNING!

After you have started the firmware installation process, do *not* interrupt the process. Do not try to go online, turn off the wireless VPN firewall, or do anything else to the wireless VPN firewall until the wireless VPN firewall has fully rebooted.

7. When the reboot process is complete, log in to the wireless VPN firewall again. (If you can see the unit: The reboot process is complete when the Test LED on the front panel goes off.)
8. Select **Monitoring**. The Router Status screen displays, showing the new firmware version in the System Info section of the screen.

Note: In some cases, such as a major upgrade, it might be necessary to erase the configuration and manually reconfigure your wireless VPN firewall after upgrading it. See the firmware release notes that NETGEAR makes available.

Configure Date and Time Service

Configure date, time, and NTP server designations on the System Date & Time screen. Network Time Protocol (NTP) is a protocol that is used to synchronize computer clock times in a network of computers. Setting the correct system time and time zone ensures that the date and time recorded in the wireless VPN firewall logs and reports are accurate.

➢ **To set time, date, and NTP servers:**

1. Select **Administration > Time Zone**. The Time Zone screen displays:

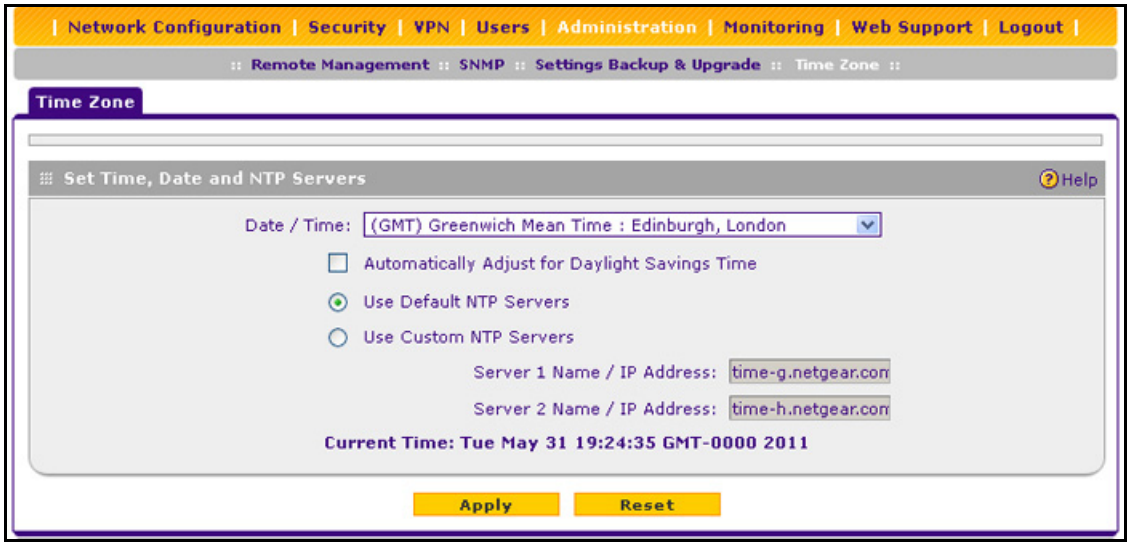

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
Remote Management :: SNMP :: Settings Backup & Upgrade :: Time Zone
Time Zone
Set Time, Date and NTP Servers
Help
Date / Time: (GMT) Greenwich Mean Time : Edinburgh, London
Automatically Adjust for Daylight Savings Time
Use Default NTP Servers
Use Custom NTP Servers
Server 1 Name / IP Address: time-g.netgear.com
Server 2 Name / IP Address: time-h.netgear.com
Current Time: Tue May 31 19:24:35 GMT-0000 2011
Apply
Reset

Figure 167.

The bottom of the screen displays the current weekday, date, time, time zone, and year (in the example in the previous figure: Current Time: Tue May 31 19:24:35 GMT-0000 2011).

2. Enter the settings as explained in the following table:

Table 72. Time Zone screen settings

Setting	Description	
Date/Time	From the drop-down list, select the local time zone in which the wireless VPN firewall operates. The correct time zone is required in order for scheduling to work correctly. The wireless VPN firewall includes a real-time clock (RTC), which it uses for scheduling.	
Automatically Adjust for Daylight Savings Time	If daylight savings time is supported in your region, select the **Automatically Adjust for Daylight Savings Time** check box.	
NTP Server (default or custom)	From the drop-down list, select an NTP server: • **Use Default NTP Servers**. The wireless VPN firewall regularly updates its RTC by contacting a default NETGEAR NTP server on the Internet. • **Use Custom NTP Servers**. The wireless VPN firewall regularly updates its RTC by contacting one of two custom NTP servers (primary and backup), both of which you need to specify in the fields that become available with this selection. **Note:** If you select the Use Custom NTP Servers option but leave either the Server 1 or Server 2 field blank, both fields are set to the default NETGEAR NTP servers. **Note:** A list of public NTP servers is available at *http://support.ntp.org/bin/view/Servers/WebHome*.	
	Server 1 Name / IP Address	Enter the IP address or host name of the primary NTP server.
	Server 2 Name / IP Address	Enter the IP address or host name of the backup NTP server.

3. Click **Apply** to save your settings.

Note: If you select the default NTP servers or if you enter a custom server FQDN, the wireless VPN firewall determines the IP address of the NTP server by performing a DNS lookup. Before the wireless VPN firewall can perform this lookup, you need to configure a DNS server address on the Broadband ISP Settings screen (see *Manually Configure an IPv4 Internet Connection* on page 27.)

Monitor System Access and Performance 10

This chapter describes the system-monitoring features of the wireless VPN firewall. You can be alerted to important events such WAN traffic limits reached, login failures, and attacks. You can also view status information about the firewall, WAN ports, LAN ports, active VPN users and tunnels, and more. In addition, the diagnostics utilities are described. This chapter contains the following sections:

- *Enable the WAN Traffic Meter*
- *Configure Logging, Alerts, and Event Notifications*
- *View Status Screens*
- *Diagnostics Utilities*

> **Note:** All log and report functions that are part of the Firewall Logs & E-mail screen and some of the functions that are part of the Diagnostics screen require that you configure the email notification server—see *Configure Logging, Alerts, and Event Notifications* on page 293.

Enable the WAN Traffic Meter

If your ISP charges by traffic volume over a given period of time, or if you want to study traffic types over a period of time, you can activate the traffic meter for the WAN port.

➢ **To monitor traffic limits on each of the WAN ports:**

1. Select **Monitoring > Traffic Meter**. The Broadband Traffic Meter screen displays.

   The Internet Traffic Statistics section in the lower part of the screen displays statistics on Internet traffic through the WAN port. If you have not enabled the traffic meter, these statistics are not available.

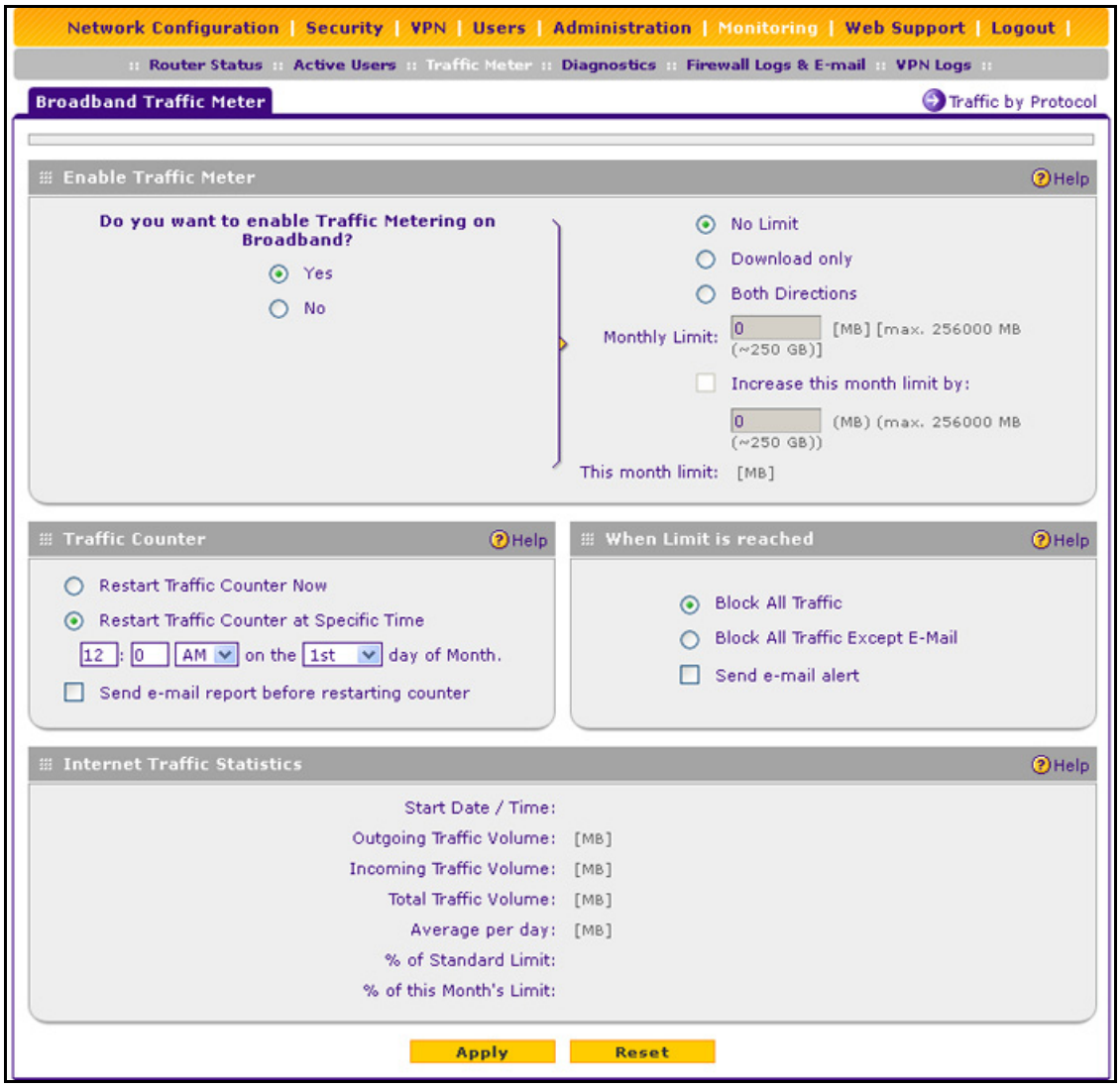

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Router Status :: Active Users :: Traffic Meter :: Diagnostics :: Firewall Logs & E-mail :: VPN Logs ::
Broadband Traffic Meter
Traffic by Protocol
Enable Traffic Meter
Help
Do you want to enable Traffic Metering on Broadband?
Yes
No
No Limit
Download only
Both Directions
Monthly Limit: 0 [MB] [max. 256000 MB (~250 GB)]
Increase this month limit by:
0 (MB) (max. 256000 MB (~250 GB))
This month limit: [MB]
Traffic Counter
Help
Restart Traffic Counter Now
Restart Traffic Counter at Specific Time
12 : 0 AM on the 1st day of Month.
Send e-mail report before restarting counter
When Limit is reached
Help
Block All Traffic
Block All Traffic Except E-Mail
Send e-mail alert
Internet Traffic Statistics
Help
Start Date / Time:
Outgoing Traffic Volume: [MB]
Incoming Traffic Volume: [MB]
Total Traffic Volume: [MB]
Average per day: [MB]
% of Standard Limit:
% of this Month's Limit:
Apply
Reset

Figure 168.

2. Enter the settings as explained in the following table:

Table 73. Broadband Traffic Meter screen settings

Setting	Description	
Enable Traffic Meter		
Do you want to enable Traffic Metering on Broadband?	Select one of the following radio buttons to configure traffic metering: • **Yes**. Traffic metering is enabled, and the traffic meter records the volume of Internet traffic passing through the WAN interface. Complete the fields that are shown on the right side of the screen (see explanations later in this table). • **No**. Traffic metering is disabled. This is the default setting.	
	Select one of the following radio buttons to specify if or how the wireless VPN firewall applies restrictions when the traffic limit is reached: • **No Limit**. No restrictions are applied when the traffic limit is reached. • **Download only**. Restrictions are applied to incoming traffic when the traffic limit is reached. Fill in the Monthly Limit field. • **Both Directions**. Restrictions are applied to both incoming and outgoing traffic when the traffic limit is reached. Fill in the Monthly Limit field.	
	Monthly Limit	Enter the monthly traffic volume limit in MB. The default setting is 0 MB.
	Increase this month limit by	Select this check box to temporarily increase a previously specified monthly traffic volume limit, and enter the additional allowed volume in MB. The default setting is 0 MB. **Note:** When you click Apply to save these settings, this field is reset to 0 MB so that the increase is applied only once.
	This month limit	This is a nonconfigurable field that displays the total monthly traffic volume limit that is applicable to this month. This total is the sum of the monthly traffic volume and the increased traffic volume.
Traffic Counter		
Restart Traffic Counter	Select one of the following radio buttons to specify when the traffic counter restarts: • **Restart Traffic Counter Now**. Select this option, and click **Apply** at the bottom of the screen to restart the traffic counter immediately. • **Restart Traffic Counter at a Specific Time**. Restart the traffic counter at a specific time and day of the month. Fill in the time fields, and select **AM** or **PM** and the day of the month from the drop-down lists.	
Send e-mail report before restarting counter	An email report is sent immediately before the counter restarts. Ensure that emailing of logs is enabled on the Email and Syslog screen (see *Configure Logging, Alerts, and Event Notifications* on page 293).	

Table 73. Broadband Traffic Meter screen settings (continued)

Setting	Description
When Limit is reached	
Block Traffic	Select one of the following radio buttons to specify which action the wireless VPN firewall performs when the traffic limit has been reached: • **Block All Traffic**. All incoming and outgoing Internet and email traffic is blocked. • **Block All Traffic Except E-Mail**. All incoming and outgoing Internet traffic is blocked, but incoming and outgoing email traffic is still allowed.
Send e-mail alert	An email alert is sent when traffic is blocked. Ensure that emailing of logs is enabled on the Email and Syslog screen (see *Configure Logging, Alerts, and Event Notifications* on page 293).

3. Click **Apply** to save your settings.

To display a report of the Internet traffic by type, click the **Traffic by Protocol** option arrow in the upper right of the Broadband Traffic Meter screen. The Traffic by Protocol screen displays in a pop-up screen. The incoming and outgoing volume of traffic for each protocol and the total volume of traffic are displayed. Traffic counters are updated in MBs; the counter starts only when traffic passed is at least 1 MB. In addition, the pop-up screen displays the traffic meter's start and end dates.

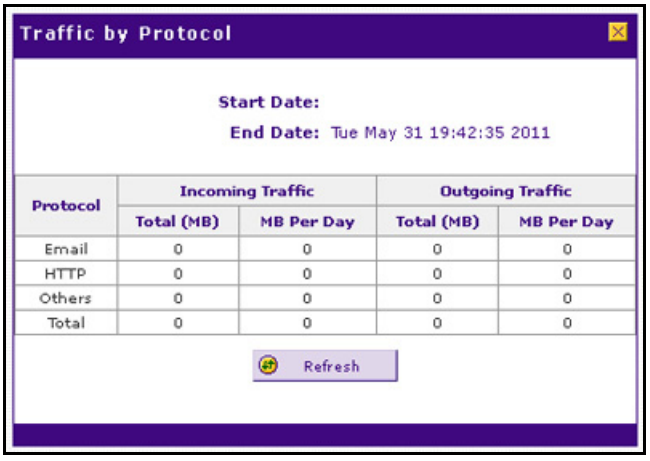


Figure 169.

Configure Logging, Alerts, and Event Notifications

You can configure the wireless VPN firewall to log routing events such as dropped and accepted packets, to log system events such as a change of time by an NTP server, secure login attempts, and reboots, and to log other events. You can also schedule logs to be sent to the administrator and enable logs to be sent to a syslog server on the network.

➤ **To configure and activate logs:**

1. Select **Monitoring > Firewall Logs & E-mail**. The Firewall Logs & E-mail screen displays:

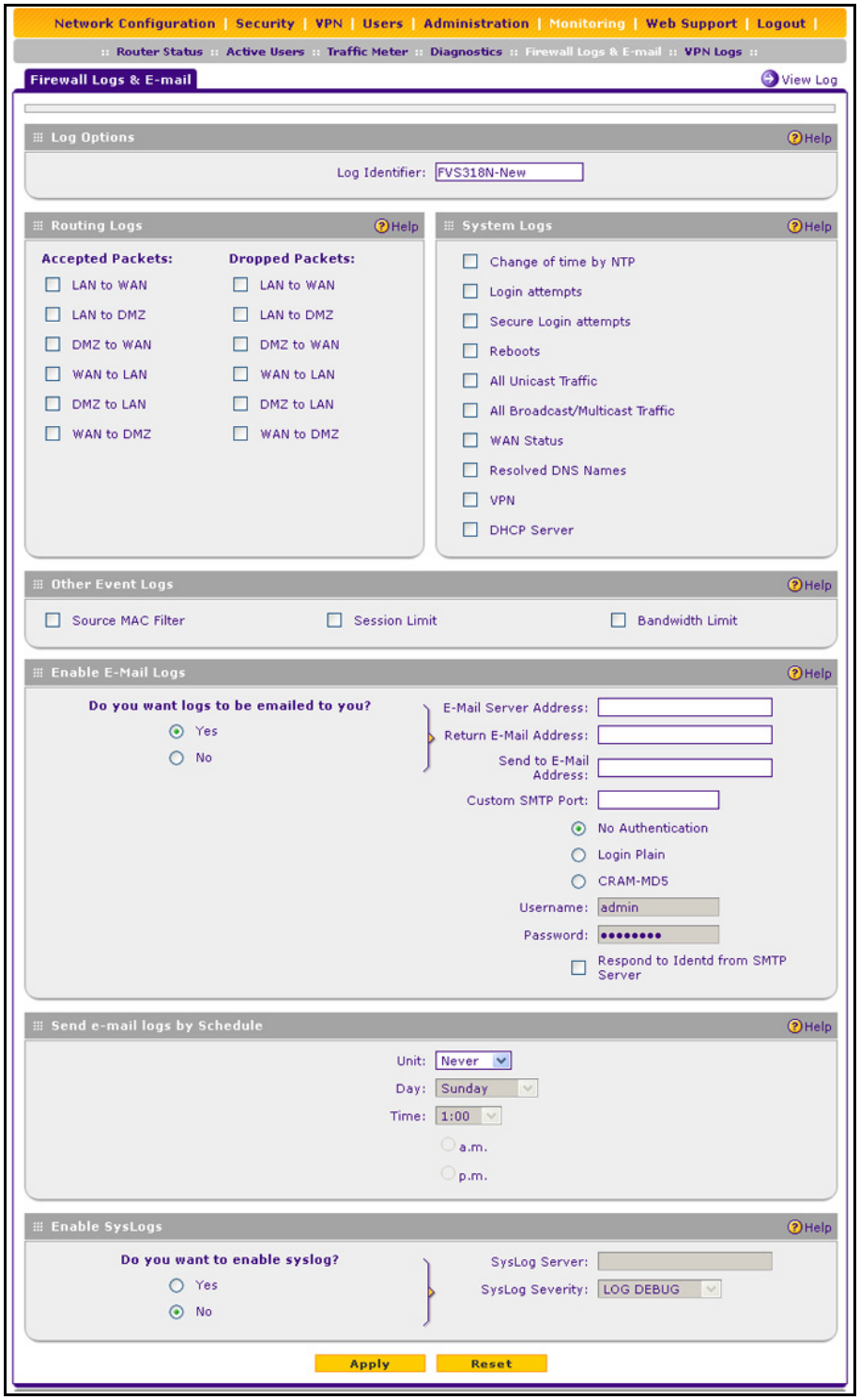


Figure 170.

2. Enter the settings as explained in the following table:

Table 74. Firewall Logs & E-mail screen settings

Setting	Description
Log Options	
Log Identifier	Enter the name of the log identifier. The identifier is appended to log messages to identify the device that sent the log messages. The default identifier is FVS318N.
Routing Logs	
In the Accepted Packets and Dropped Packets columns, select check boxes to specify which traffic is logged: • **LAN to WAN** • **LAN to DMZ** • **DMZ to WAN** • **WAN to LAN** • **DMZ to LAN** • **WAN to DMZ**	
System Logs Option	
Select the check boxes to specify which system events are logged: • **Change of Time by NTP**. Logs a message when the system time changes after a request from an NTP server. • **Login Attempts**. Logs a message when a login is attempted. Both successful and failed login attempts are logged. • **Secure Login Attempts**. Logs a message when a secure login is attempted. Both successful and failed secure login attempts are logged. • **Reboots**. Logs a message when the wireless VPN firewall has been rebooted through the web management interface. (No message is logged when the factory default Reset button has been pressed.) • **All Unicast Traffic**. All incoming unicast packets are logged. • **All Broadcast/Multicast Traffic**. All incoming broadcast and multicast packets are logged. • **WAN Status**. WAN link status-related events are logged. • **Resolved DNS Names**. All resolved DNS names are logged. • **VPN**. All VPN negotiation messages are logged. • **DHCP Server**. All DHCP server events are logged.	
Other Event Logs	
Source MAC Filter	Select this check box to log packets from MAC addresses that match the source MAC address filter settings.
Session Limit	Select this check box to log packets that are dropped because the session limit has been exceeded.
Bandwidth Limit	Select this check box to log packets that are dropped because the bandwidth limit has been exceeded.

Table 74. Firewall Logs & E-mail screen settings (continued)

Setting	Description	
Enable E-mail Logs		
Do you want logs to be emailed to you?	Select the **Yes** radio button to enable the wireless VPN firewall to email logs to a specified email address. Complete the fields that are shown on the right side of the screen. Select the **No** radio button to prevent the logs from being emailed, which is the default setting.	
	E-Mail Server Address	The IP address or Internet name of your ISP's outgoing email SMTP server. **Note:** If you leave this field blank, the wireless VPN firewall cannot send email logs and alerts.
	Return E-Mail Address	The email address of the sender for email identification purposes. For example, enter fvs_alerts@company.com.
	Send to E-Mail Address	The email address to which the logs are sent. Typically, this is the email address of the administrator.
	Custom SMTP Port	Enter the port number of the SMTP server for the outgoing email.
	Select one of the following radio buttons to specify SMTP server authentication for the outgoing email: • **No Authentication**. The SMTP server does not require authentication. • **Login Plain**. The SMTP server requires authentication with regular login. Specify the user name and password to be used for authentication. • **CRAM-MD5**. The SMTP server requires authentication with CRAM-MD5 login. Specify the user name and password to be used for authentication.	
	Username	The user name for SMTP server authentication.
	Password	The password for SMTP server authentication.
	Respond to Identd from SMTP Server	To respond to Ident protocol messages, select the **Respond to Identd from SMTP Server** check box. The Ident protocol is a relatively weak scheme to verify the sender of an email. (A common daemon program for providing the Ident service is Identd.)
Send e-mail logs by Schedule		
Unit	Enter a schedule for sending the logs. From the Unit drop-down list, select one of the following: • **Never**. No logs are sent. • **Hourly**. The logs are sent every hour. • **Daily**. The logs are sent daily. Specify the time. • **Weekly**. The logs are sent weekly. Specify the day and time.	
Day	From the Day drop-down list, select the day on which the logs are sent.	
Time	From the Time drop-down, list select the hour on which the logs are sent, and then select either the **a.m.** or **p.m.** radio button.	

Table 74. Firewall Logs & E-mail screen settings (continued)

Setting	Description	
Send Logs via Syslog		
Do you want to enable syslog?	To enable the wireless VPN firewall to send logs to a specified syslog server, select the **Yes** radio button. Complete the fields that are shown on the right side of the screen. To prevent the logs from being sent, select the **No** radio button, which is the default setting.	
	SysLog Server	The IP address or FQDN of the syslog server.
	SysLog Severity	All the logs with a severity that is equal to and above the severity that you specify are logged on the specified syslog server. For example, if you select LOG_CRITICAL as the severity, then the logs with the severities LOG_CRITICAL, LOG_ALERT, and LOG_EMERG are logged. Select one of the following syslog severities from the drop-down list: • **LOG DEBUG**. Debug-level messages. • **LOG INFO**. Informational messages. • **LOG NOTICE**. There are normal but significant conditions. • **LOG WARNING**. There are warning conditions. • **LOG ERROR**. There are error conditions. • **LOG CRITICAL**. There are critical conditions. • **LOG ALERT**. An action has to be taken immediately. • **LOG EMERG**. The wireless VPN firewall is unusable.

3. Click **Apply** to save your settings.

Note: Enabling routing and other event logs might generate a significant volume of log messages. NETGEAR recommends that you enable firewall logs for debugging purposes only.

How to Send Syslogs over a VPN Tunnel between Sites

➢ **To send syslogs from one site to another over a gateway-to-gateway VPN tunnel:**

1. At Site 1, set up a syslog server that is connected to Gateway 1.
2. Set up a VPN tunnel between Gateway 1 at Site 1 and Gateway 2 at Site 2.
3. Change the remote IP address in the VPN policy on Gateway 1 to the WAN IP address of Gateway 2.
4. Change the local IP address in the VPN policy on Gateway 2 to the WAN IP address of Gateway 2.
5. At Site 2, specify that Gateway 2 should send the syslogs to the syslog server at Site 1.

This section describes steps 2 through 4, using the topology that is described in the following table:

Type of address	Gateway 1 at Site 1	Gateway 2 at Site 2
WAN IP address	10.0.0.1	10.0.0.2
LAN IP address	192.168.10.0	192.168.20.0
LAN subnet mask	255.255.255.0	255.255.255.0
LAN IP address syslog server	192.168.10.2	not applicable

Configure Gateway 1 at Site 1

➢ **To create a gateway-to-gateway VPN tunnel to Gateway 2, using the IPSec VPN wizard:**

1. Select **VPN > IPSec VPN > VPN Wizard**. The VPN Wizard screen displays.
2. Configure a gateway-to-gateway VPN tunnel using the following information:
   - Connection name. Any name of your choice
   - Pre-shared key. Any key of your choice
   - Remote WAN IP address. 10.0.0.2
   - Local WAN IP address. 10.0.0.1
   - Remote LAN IP Address. 192.168.20.0
   - Remote LAN subnet mask. 255.255.255.0
3. Click **Apply** to save the settings.

➢ **To change the remote IP address in the VPN policy:**

1. Select **VPN > IPSec VPN > VPN Policies**. The VPN Policy screen displays.
2. Next to the policy name for the Gateway 1–to–Gateway 2 autopolicy, click **Edit**. The Edit VPN Policy screen displays.
3. In the General section of the screen, clear the **Enable NetBIOS** check box.
4. In the Traffic Selector section of the screen, make the following changes:
   - From the Remote IP drop-down list, select **Single**.
   - In the Start IP fields, type **10.0.0.2**, which is the WAN IP address of Gateway 2.
5. Click **Apply** to save the settings.

Configure Gateway 2 at Site 2

➢ **To create a gateway-to-gateway VPN tunnel to Gateway 1, using the IPSec VPN wizard:**

1. Select **VPN > IPSec VPN > VPN Wizard**. The VPN Wizard screen displays.

2. Configure a gateway-to-gateway VPN tunnel using the following information:
   - Connection name. Any name of your choice
   - Pre-shared key. The same key as you configured on Gateway 1
   - Remote WAN IP address. 10.0.0.1
   - Local WAN IP address. 10.0.0.2
   - Remote LAN IP Address. 192.168.10.0
   - Remote LAN subnet mask. 255.255.255.0
3. Click **Apply** to save the settings.

➢ **To change the local IP address in the VPN policy:**

1. Select **VPN > IPSec VPN > VPN Policies**. The VPN Policy screen displays.
2. Next to the policy name for the Gateway 2–to–Gateway 1 autopolicy, click **Edit**. The Edit VPN Policy screen displays.
3. In the General section of the screen, clear the **Enable NetBIOS** check box.
4. In the Traffic Selector section of the screen, make the following changes:
   - From the Local IP drop-down list, select **Single**.
   - In the Start IP fields, type **10.0.0.2**, which is the WAN IP address of Gateway 2.
5. Click **Apply** to save the settings.

➢ **To specify the syslog server that is connected to Gateway 1:**

1. Select **Monitoring > Firewall Logs & E-mail**. The Firewall Logs & E-mail screen displays.
2. Enable the syslog server and specify its IP address at Site 1. Enter **192.168.10.2** as the IP address.
3. Click **Apply** to save the settings.

Note: The VPN tunnel should be established automatically, and the syslogs should be sent to the syslog server at Site 1. You can use the IPSec VPN Connection Status screen to verify the connection.

View Status Screens

The wireless VPN firewall provides real-time information in a variety of status screens that are described in the following sections:

- *View the System Status*
- *View the VPN Connection Status and L2TP Users*
- *View the VPN Logs*
- *View the Port Triggering Status*
- *View the WAN Port Status*
- *View the Attached Devices and the DHCP Log*

View the System Status

When you start up the wireless VPN firewall, the default screen that displays is the Router Status screen.

The Router Status screen and Detailed Status screen provide real-time information about the following important components of the wireless VPN firewall:

- Firmware version
- Both IPv4 and IPv6 WAN and LAN port information
- Wireless information
- Interface statistics
- VLAN status, including port memberships

These status screens are described in the following sections:

- *Router Status Screen*
- *Router Statistics Screen*
- *Detailed Status Screen*

Router Status Screen

➢ **To view the Router Status screen:**

Select **Monitoring > Router Status**. The Router Status screen displays:

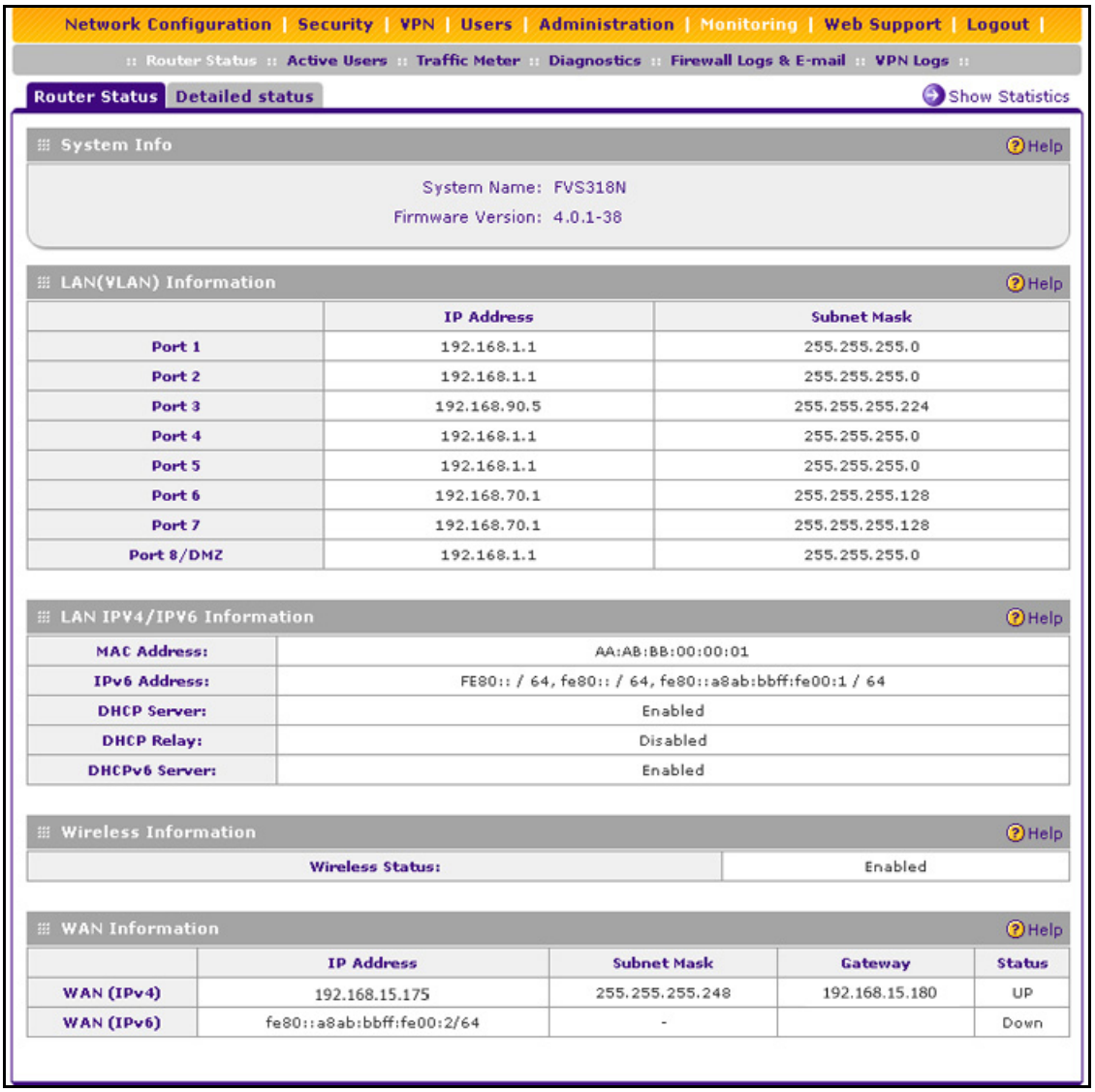


Figure 171.

The following table explains the fields of the Router Status screen:

Table 75. Router Status screen information

Item	Description
System Info	
System Name	The NETGEAR system name.
Firmware Version	The currently installed firmware version.
LAN (VLAN) Information	
For each of the LAN ports, the screen shows the IP address and subnet mask. For more detailed information, see *Table 77* on page 305.	

Table 75. Router Status screen information (continued)

Item	Description
LAN IPv4/IPv6 Information	
MAC Address	The MAC address of the wireless VPN firewall.
IPv6 Address	The IPv6 address that is assigned to the wireless VPN firewall. For information about configuring the IPv6 address, see *Configure the IPv6 Internet Connection* on page 32.
DHCP Server	The status of the IPv4 DHCP server (Enabled or Disabled). For information about configuring the IPv4 DHCP server, see *Configure a VLAN Profile* on page 51.
DHCP Relay	The status of the IPv4 DHCP relay (Enabled or Disabled). For information about configuring the IPv4 DHCP relay, see *Configure a VLAN Profile* on page 51.
DHCPv6 Server	The status of the DHCPv6 server (Enabled or Disabled). For information about configuring the DHCPv6 server, see *Configure IPv6 LAN Settings* on page 64.
Wireless Information	
Wireless Status	The status of the wireless access point (Enabled or Disabled).
WAN Information	
WAN (IPv4)	The screen shows the IPv4 address, subnet mask, gateway, and status of the port (UP or Down). For more detailed information, see *Table 77* on page 305.
WAN (IPv6)	The screen shows the IPv6 address, gateway, and status of the port (UP or Down). For more detailed information, see *Table 77* on page 305.

Router Statistics Screen

➢ **To view the Router Statistics screen:**

1. Select **Monitoring > Router Status**. The Router Status screen displays (see the previous figure).
2. Click the **Show Statistics** option arrow in the upper right of the Router Status screen. The Router Statistics screen displays:

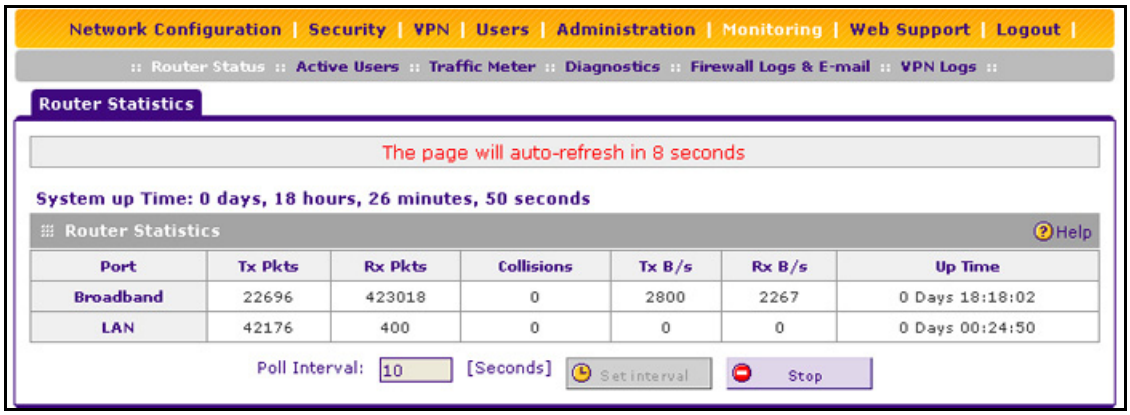

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Router Status :: Active Users :: Traffic Meter :: Diagnostics :: Firewall Logs & E-mail :: VPN Logs ::
Router Statistics
The page will auto-refresh in 8 seconds
System up Time: 0 days, 18 hours, 26 minutes, 50 seconds
Router Statistics
Help
Port | Tx Pkts | Rx Pkts | Collisions | Tx B/s | Rx B/s | Up Time
Broadband | 22696 | 423018 | 0 | 2800 | 2267 | 0 Days 18:18:02
LAN | 42176 | 400 | 0 | 0 | 0 | 0 Days 00:24:50
Poll Interval: 10 [Seconds] Set Interval Stop

Figure 172.

The following table explains the fields of the Router Statistics screen.

To change the poll interval period, enter a new value (in seconds) in the Poll Interval field, and then click **Set interval**. To stop polling, click **Stop**.

Table 76. Router Statistics screen information

Item	Description
System up Time. The period since the last time that the wireless VPN firewall was started up.	
Router Statistics	
For the broadband (WAN) interface and for all LAN interfaces combined, the following statistics are displayed:	
Tx Pkts	The number of packets transmitted on the port in bytes.
Rx Pxts	The number of packets received on the port in bytes.
Collisions	The number of signal collisions that have occurred on the port. A collision occurs when the port attempts to send data at the same time as a port on the other router or computer that is connected to this port.
Tx B/s	The number of bytes transmitted per second on the port.
Rx B/s	The number of bytes received per second on the port.
Up Time	The period that the port has been active since it was restarted.

Detailed Status Screen

To view the Detailed Status screen, select **Monitoring > System Status > Detailed Status**. The Detailed Status screen displays:

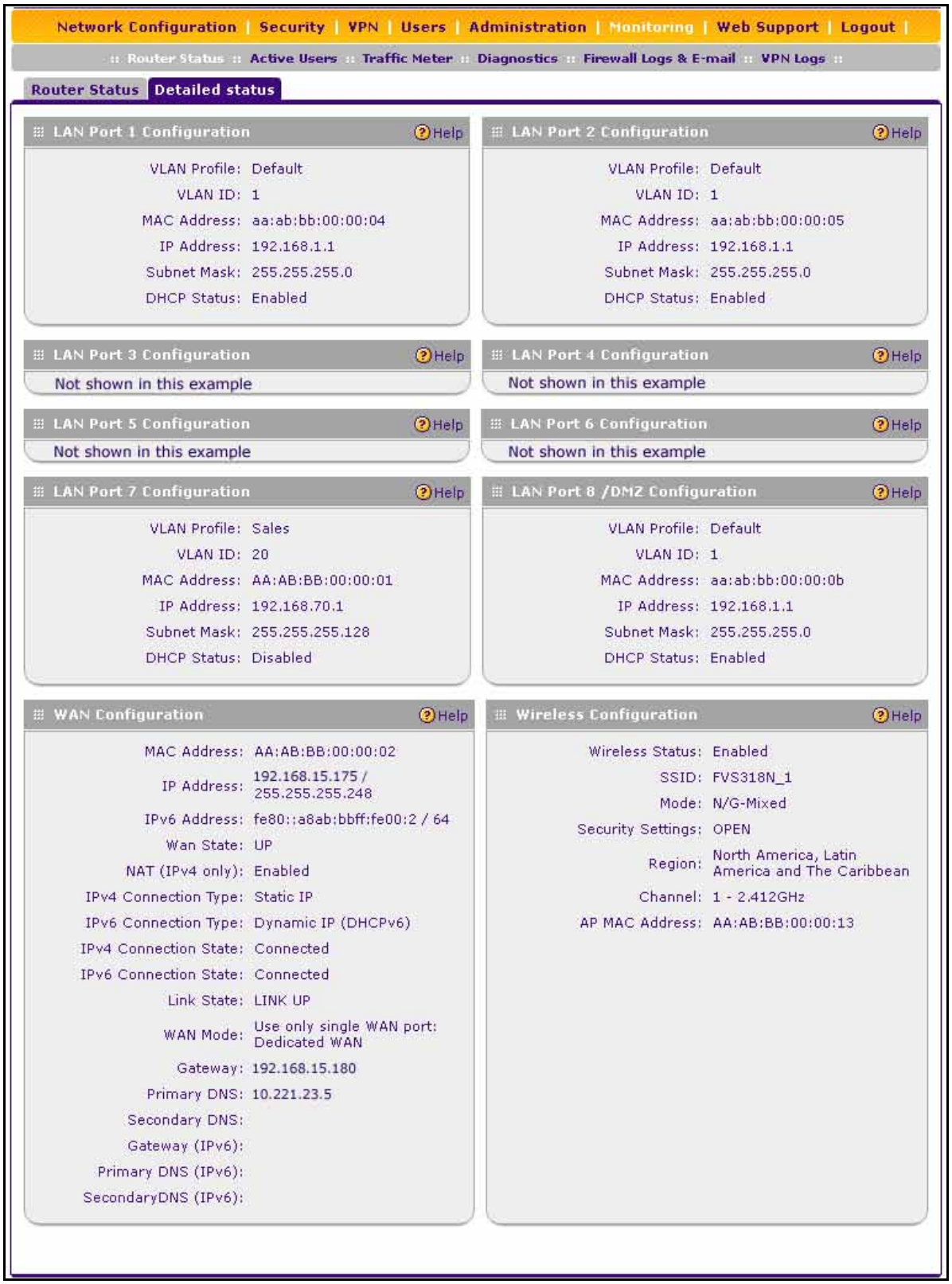

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Router Status :: Active Users :: Traffic Meter :: Diagnostics :: Firewall Logs & E-mail :: VPN Logs ::
Router Status
Detailed status
LAN Port 1 Configuration
Help
VLAN Profile: Default
VLAN ID: 1
MAC Address: aa:ab:bb:00:00:04
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
DHCP Status: Enabled
LAN Port 2 Configuration
Help
VLAN Profile: Default
VLAN ID: 1
MAC Address: aa:ab:bb:00:00:05
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
DHCP Status: Enabled
LAN Port 3 Configuration
Help
Not shown in this example
LAN Port 4 Configuration
Help
Not shown in this example
LAN Port 5 Configuration
Help
Not shown in this example
LAN Port 6 Configuration
Help
Not shown in this example
LAN Port 7 Configuration
Help
VLAN Profile: Sales
VLAN ID: 20
MAC Address: AA:AB:BB:00:00:01
IP Address: 192.168.70.1
Subnet Mask: 255.255.255.128
DHCP Status: Disabled
LAN Port 8 /DMZ Configuration
Help
VLAN Profile: Default
VLAN ID: 1
MAC Address: aa:ab:bb:00:00:0b
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
DHCP Status: Enabled
WAN Configuration
Help
MAC Address: AA:AB:BB:00:00:02
IP Address: 192.168.15.175 / 255.255.255.248
IPv6 Address: fe80::a8ab:bbff:fe00:2 / 64
Wan State: UP
NAT (IPv4 only): Enabled
IPv4 Connection Type: Static IP
IPv6 Connection Type: Dynamic IP (DHCPv6)
IPv4 Connection State: Connected
IPv6 Connection State: Connected
Link State: LINK UP
WAN Mode: Use only single WAN port: Dedicated WAN
Gateway: 192.168.15.180
Primary DNS: 10.221.23.5
Secondary DNS:
Gateway (IPv6):
Primary DNS (IPv6):
SecondaryDNS (IPv6):
Wireless Configuration
Help
Wireless Status: Enabled
SSID: FVS318N_1
Mode: N/G-Mixed
Security Settings: OPEN
Region: North America, Latin America and The Caribbean
Channel: 1 - 2.412GHz
AP MAC Address: AA:AB:BB:00:00:13

Figure 173.

The following table explains the fields of the Detailed Status screen:

Table 77. Detailed Status screen information

Item	Description
LAN Port Configuration The following fields are shown for each of the LAN ports.	
VLAN Profile	The name of the VLAN profile that you assigned to this port on the LAN Setup screen (see *Assign and Manage VLAN Profiles* on page 48). If the VLAN is not enabled on this port, the default profile (with VLAN ID 1) is assigned automatically.
VLAN ID	The VLAN ID that you assigned to this port on the Add VLAN Profile screen (see *Configure a VLAN Profile* on page 51). If the default VLAN profile is used, the VLAN ID is 1, which means that all tagged and untagged traffic can pass on this port.
MAC Address	The MAC address for this port. **Note:** All LAN ports that are part of the default VLAN share the same MAC address unless you have specified that each VLAN needs to be assigned a unique MAC address (see *Configure VLAN MAC Addresses and LAN Advanced Settings* on page 56). **Note:** LAN ports that have an IPv4 address that differs from the default VLAN can share the same MAC address as the default VLAN. **Note:** LAN port 8 can be assigned as the DMZ port, in which case its VLAN ID is 4094. For information about configuring the DMZ port, see *Configure and Enable the DMZ Port for IPv4 Traffic* on page 72.
IP Address	The IP address for this port. If the port is part of the default VLAN, the IP address is the default LAN IP address (192.168.1.1). For information about configuring VLAN profiles, see *Configure a VLAN Profile* on page 51.
Subnet Mask	The subnet mask for this port. If the port is part of the default VLAN, the subnet mask is the default LAN IP subnet mask (255.255.255.0). For information about configuring VLAN profiles, see *Configure a VLAN Profile* on page 51.
DHCP Status	The status of the IPv4 DHCP server for the VLAN (Enabled or Disabled). For information about enabling DHCP for VLANs, see *Configure a VLAN Profile* on page 51.
WAN Configuration	
MAC Address	The default MAC address for the port or the MAC address that you have specified on the Broadband Advanced Options screen for the port. For information about configuring the MAC address, see *Configure Advanced WAN Options and Other Tasks* on page 43.
IP Address	The IPv4 address and subnet mask of the WAN port. For information about configuring the IPv4 address of the WAN port, see *Configure the IPv4 Internet Connection* on page 24.
IPv6 Address	The IPv6 address of the WAN port. For information about configuring the IPv4 address of the WAN port, see *Configure the IPv6 Internet Connection* on page 32.
WAN State	The WAN state can be either UP or DOWN, depending on whether or not the port is connected to the Internet.

Table 77. Detailed Status screen information (continued)

Item	Description	
NAT (IPv4 only)	The NAT state can be either Enabled or Disabled, depending on whether or not NAT is enabled (see *Network Address Translation* on page 31) or classical routing is enabled (see *Classical Routing* on page 31).	
IPv4 Connection Type	The connection type can be Static IP, DHCP, PPPoE, or PPTP, depending on whether the WAN address is obtained dynamically through a DHCP server or assigned statically by you. For information about connection types, see *Configure the IPv4 Internet Connection* on page 24.	
IPv6 Connection Type	The connection type can be Static IPv6 or Dynamic IP (DHCPv6), depending on whether the WAN address is obtained dynamically through a DHCP server or assigned statically by you. For information about connection types, see *Configure the IPv6 Internet Connection* on page 32.	
IPv4 Connection State	The IPv4 connection state can be either Connected or Not Connected, depending on whether or not the WAN interface is connected to the Internet over an IPv4 address. For information about configuring the IPv4 address of the WAN port, see *Configure the IPv4 Internet Connection* on page 24.	
IPv6 Connection State	The IPv6 connection state can be either Connected or Not Connected, depending on whether or not the WAN interface is connected to the Internet over an IPv6 address. For information about configuring the IPv6 address of the WAN port, see *Configure the IPv6 Internet Connection* on page 32.	
Link State	The link state can be either LINK UP or LINK DOWN, depending on whether or not the WAN port is physically connected to a modem or router. For information about connecting a WAN port, see the *ProSafe Wireless-N 8-Port Gigabit VPN Firewall FVS318N Installation Manual*.	
WAN Mode	This is a fixed field that states: Use only single WAN port: Dedicated WAN.	
Gateway	The IP address of the gateway.	These IPv4 settings are either obtained dynamically from your ISP or specified by you on the Broadband ISP Settings (IPv4) screen (see *Manually Configure an IPv4 Internet Connection* on page 27).
Primary DNS Server	The IP address of the primary DNS server.	
Secondary DNS Server	The IP address of the secondary DNS server.	
Gateway (IPv6)	The IP address of the gateway.	These IPv6 settings are either obtained dynamically from your ISP or specified by you on the Broadband ISP Settings (IPv6) screen (see *Manually Configure an IPv6 Internet Connection* on page 34).
Primary DNS Server (IPv6)	The IP address of the primary DNS server.	
Secondary DNS Server (IPv6)	The IP address of the secondary DNS server.	

Table 77. Detailed Status screen information (continued)

Item	Description
Wireless Configuration	
Wireless Status	The wireless status can be Enabled or Disabled, depending on whether or not the default virtual access point is enabled. For information about enabling the default virtual access point, see *Configure Virtual Access Points* on page 98.
SSID	The SSID of the default profile. For information about how to configure the SSID, see *Configure and Enable Wireless Security Profiles* on page 93.
Mode	The wireless mode of the radio. For information about how to configure the wireless mode, see *Configure the Basic Radio Settings* on page 86.
Security Settings	The security settings of the default profile. For information about how to configure the security profile, see *Configure and Enable Wireless Security Profiles* on page 93.
Region	The region that is assigned to the radio. For information about how to configure the region, see *Configure the Basic Radio Settings* on page 86.
Channel	The active channel on the radio. For information about how to configure the channel, see *Configure the Basic Radio Settings* on page 86.
AP MAC Address	The MAC address of the radio or default virtual access point. If the default virtual access point is disabled, the MAC address is not displayed.

View the VPN Connection Status and L2TP Users

The Connection Status screens displays a list of IPSec VPN connections, SSL VPN connections, and L2TP users who are currently logged in to the wireless VPN firewall.

➤ **To view the active IPSec VPN connections:**

Select **VPN > Connection Status > IPSec VPN Connection Status**. The IPSec VPN Connection Status screen displays:

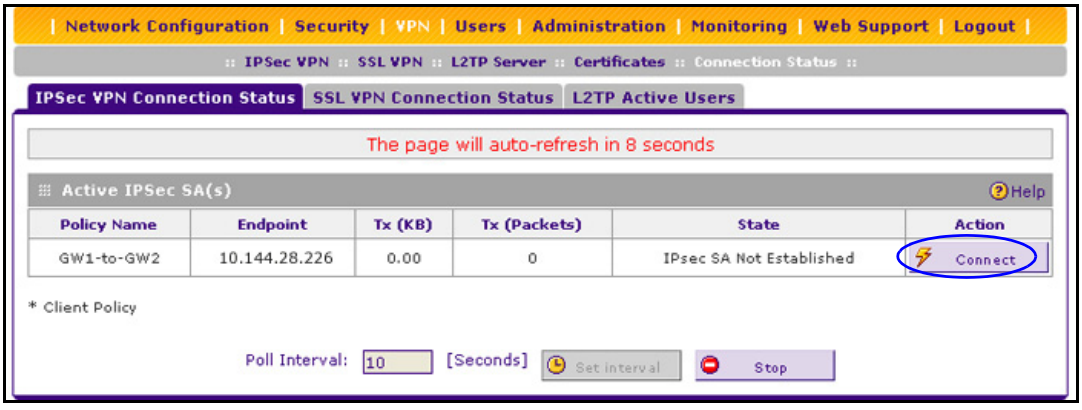


Figure 174.

The policy name, the endpoint's IP address, the amount of data and number of packets transmitted, and the state of the connection are listed in the table.

To disconnect an active connection, click the **Disconnect** table button to the right of the policy's table entry.

- **To view the active SSL VPN connections:**

Select **VPN > Connection Status > SSL VPN Connection Status**. The SSL VPN Connection Status screen displays:

Figure 175.

The active user's user name, group, and IP address are listed in the table with a time stamp indicating the time and date that the user connected.

To disconnect an active user, click the **Disconnect** table button to the right of the user's table entry.

- **To view the active L2TP tunnel users:**

Select **VPN > Connection Status > L2TP Active Users**. The L2TP Active Users screen displays:

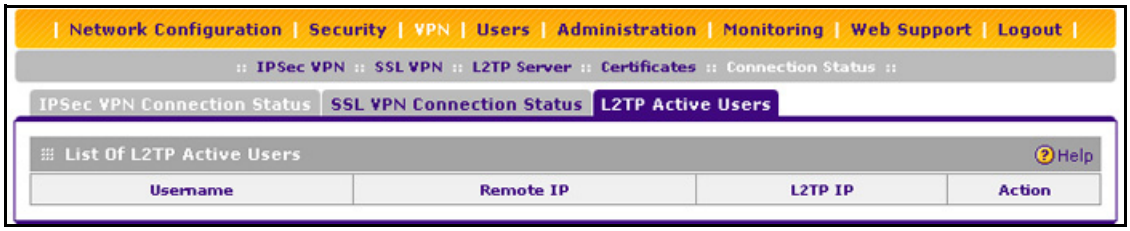

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
:: IPSec VPN :: SSL VPN :: L2TP Server :: Certificates :: Connection Status ::
IPSec VPN Connection Status
SSL VPN Connection Status
L2TP Active Users
List Of L2TP Active Users
Help
Username
Remote IP
L2TP IP
Action

Figure 176.

The active user name, client's IP address on the remote LAC, and IP address that is assigned by the L2TP server on the wireless VPN firewall are listed in the table.

To disconnect an active user, click the **Disconnect** table button to the right of the user's table entry.

View the VPN Logs

➢ **To display the IPSec VPN log:**

Select **Monitoring > VPN Logs > IPSec VPN Logs**. The IPSec VPN Logs screen displays.

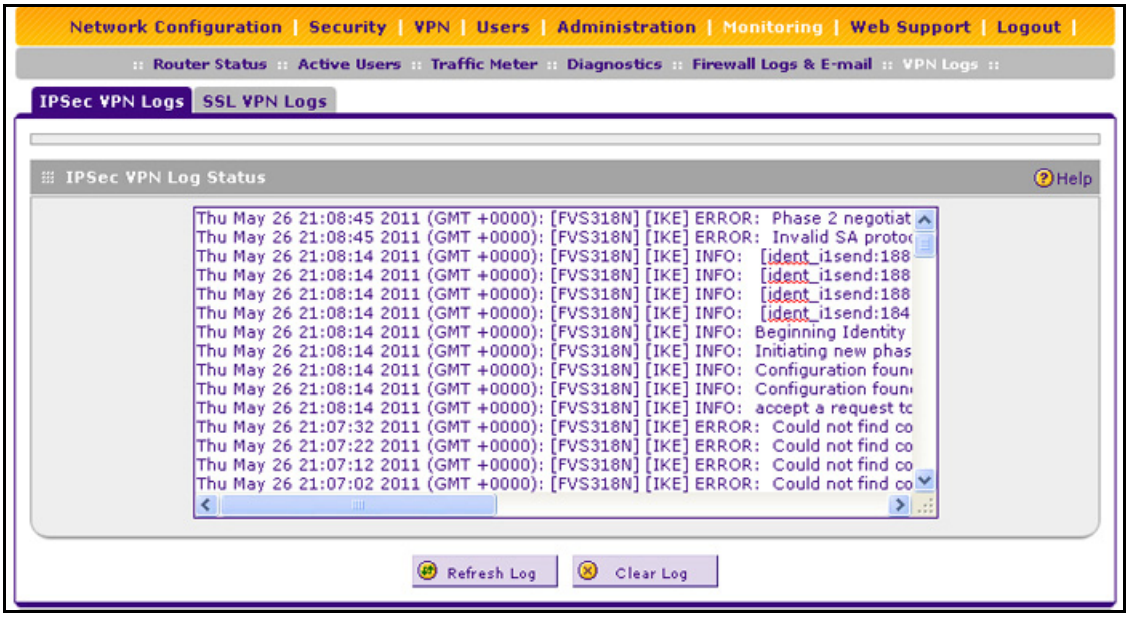

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Router Status :: Active Users :: Traffic Meter :: Diagnostics :: Firewall Logs & E-mail :: VPN Logs ::
IPSec VPN Logs
SSL VPN Logs
IPSec VPN Log Status
Help
Thu May 26 21:08:45 2011 (GMT +0000): [FVS318N] [IKE] ERROR: Phase 2 negotiat
Thu May 26 21:08:45 2011 (GMT +0000): [FVS318N] [IKE] ERROR: Invalid SA protoc
Thu May 26 21:08:14 2011 (GMT +0000): [FVS318N] [IKE] INFO: [ident_i1send:188
Thu May 26 21:08:14 2011 (GMT +0000): [FVS318N] [IKE] INFO: [ident_i1send:188
Thu May 26 21:08:14 2011 (GMT +0000): [FVS318N] [IKE] INFO: [ident_i1send:188
Thu May 26 21:08:14 2011 (GMT +0000): [FVS318N] [IKE] INFO: [ident_i1send:184
Thu May 26 21:08:14 2011 (GMT +0000): [FVS318N] [IKE] INFO: Beginning Identity
Thu May 26 21:08:14 2011 (GMT +0000): [FVS318N] [IKE] INFO: Initiating new phas
Thu May 26 21:08:14 2011 (GMT +0000): [FVS318N] [IKE] INFO: Configuration foun
Thu May 26 21:08:14 2011 (GMT +0000): [FVS318N] [IKE] INFO: Configuration foun
Thu May 26 21:08:14 2011 (GMT +0000): [FVS318N] [IKE] INFO: accept a request tc
Thu May 26 21:07:32 2011 (GMT +0000): [FVS318N] [IKE] ERROR: Could not find co
Thu May 26 21:07:22 2011 (GMT +0000): [FVS318N] [IKE] ERROR: Could not find co
Thu May 26 21:07:12 2011 (GMT +0000): [FVS318N] [IKE] ERROR: Could not find co
Thu May 26 21:07:02 2011 (GMT +0000): [FVS318N] [IKE] ERROR: Could not find co
Refresh Log
Clear Log

Figure 177.

➢ **To display the SSL VPN log:**

Select **Monitoring > VPN Logs > SSL VPN Logs**. The SSL VPN Logs screen displays:

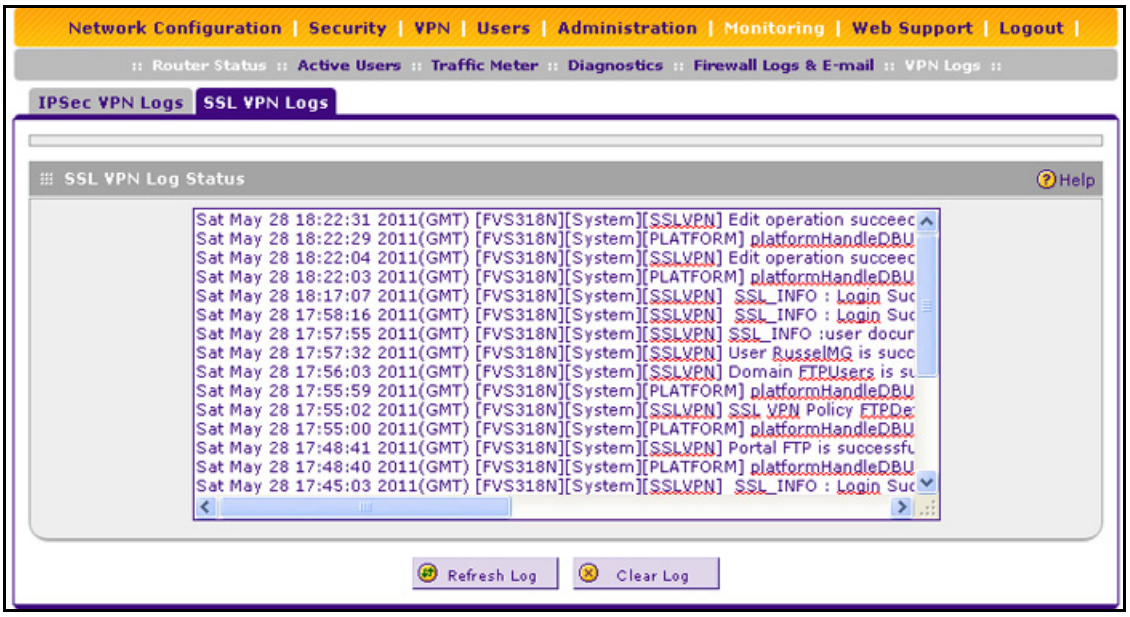

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Router Status :: Active Users :: Traffic Meter :: Diagnostics :: Firewall Logs & E-mail :: VPN Logs ::
IPSec VPN Logs
SSL VPN Logs
SSL VPN Log Status
Help
Sat May 28 18:22:31 2011(GMT) [FVS318N][System][SSLVPN] Edit operation succeec
Sat May 28 18:22:29 2011(GMT) [FVS318N][System][PLATFORM] platformHandleDBU
Sat May 28 18:22:04 2011(GMT) [FVS318N][System][SSLVPN] Edit operation succeec
Sat May 28 18:22:03 2011(GMT) [FVS318N][System][PLATFORM] platformHandleDBU
Sat May 28 18:17:07 2011(GMT) [FVS318N][System][SSLVPN] SSL_INFO : Login Suc
Sat May 28 17:58:16 2011(GMT) [FVS318N][System][SSLVPN] SSL_INFO : Login Suc
Sat May 28 17:57:55 2011(GMT) [FVS318N][System][SSLVPN] SSL_INFO :user docur
Sat May 28 17:57:32 2011(GMT) [FVS318N][System][SSLVPN] User RusselMG is succ
Sat May 28 17:56:03 2011(GMT) [FVS318N][System][SSLVPN] Domain FTPUsers is su
Sat May 28 17:55:59 2011(GMT) [FVS318N][System][PLATFORM] platformHandleDBU
Sat May 28 17:55:02 2011(GMT) [FVS318N][System][SSLVPN] SSL VPN Policy FTPDe
Sat May 28 17:55:00 2011(GMT) [FVS318N][System][PLATFORM] platformHandleDBU
Sat May 28 17:48:41 2011(GMT) [FVS318N][System][SSLVPN] Portal FTP is successfu
Sat May 28 17:48:40 2011(GMT) [FVS318N][System][PLATFORM] platformHandleDBU
Sat May 28 17:45:03 2011(GMT) [FVS318N][System][SSLVPN] SSL_INFO : Login Suc
Refresh Log
Clear Log

Figure 178.

View the Port Triggering Status

➢ **To view the status of the port-triggering feature:**

1. Select **Security > Port Triggering**. The Port Triggering screen displays. (The following figure shows one rule in the Port Triggering Rules table as an example.)

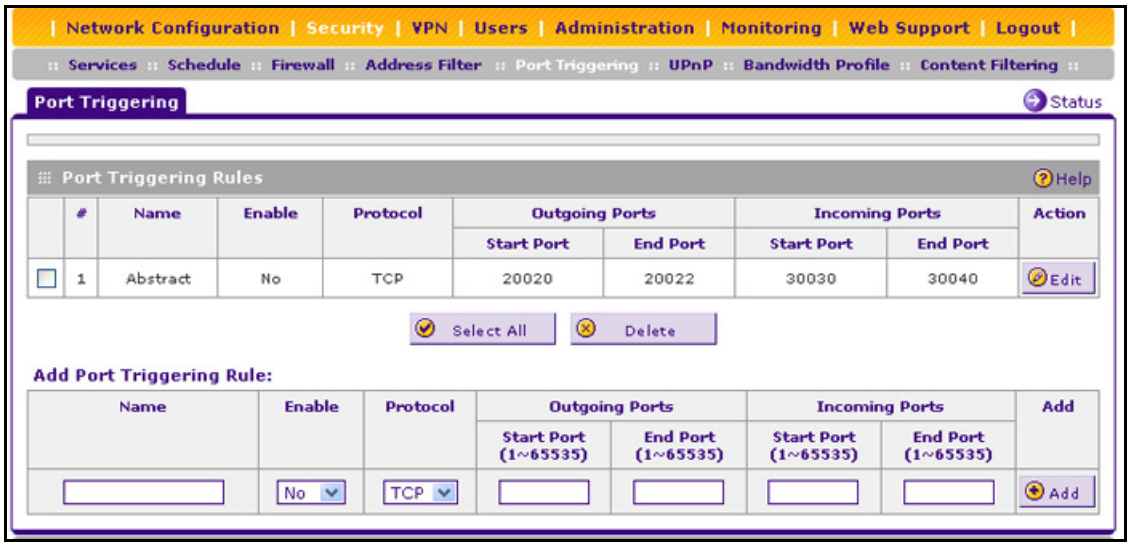

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering
Port Triggering
Status
Port Triggering Rules
Help
Name Enable Protocol Outgoing Ports Incoming Ports Action
Start Port End Port Start Port End Port
1 Abstract No TCP 20020 20022 30030 30040 Edit
Select All
Delete
Add Port Triggering Rule:
Name Enable Protocol Outgoing Ports Incoming Ports Add
Start Port (1~65535) End Port (1~65535) Start Port (1~65535) End Port (1~65535)
No
TCP
Add

Figure 179.

2. Click the **Status** option arrow in the upper right of the Port Triggering screen. The Port Triggering Status screen displays in a pop-up screen.

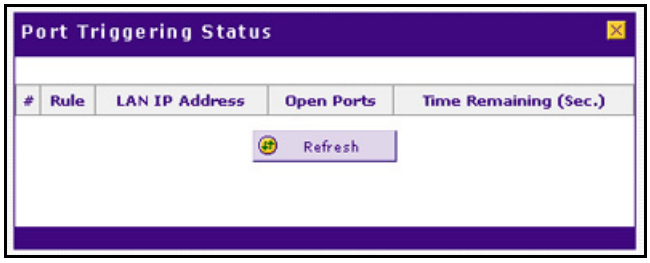


Figure 180.

The Port Triggering Status screen displays the information that is described in the following table:

Table 78. Port Triggering Status screen information

Item	Description
#	The sequence number of the rule onscreen.
Rule	The name of the port-triggering rule that is associated with this entry.
LAN IP Address	The IP address of the computer or device that is currently using this rule.

Table 78. Port Triggering Status screen information (continued)

Item	Description
Open Ports	The incoming ports that are associated with this rule. Incoming traffic using one of these ports is sent to the IP address that is listed in the LAN IP Address field.
Time Remaining	The time remaining before this rule is released and made available for other computers or devices. This timer is restarted when incoming or outgoing traffic is received.

View the WAN Port Status

You can view the status of the IPv4 and IPv6 WAN connections, the DNS servers, and the DHCP servers.

IPv4 WAN Port Status

➢ **To view the IPv4 status of the WAN port:**

1. Select **Network Configuration > WAN Settings > Broadband ISP Settings (IPv4)**. The Broadband ISP Settings (IPv4) screen displays (see *Figure 9* on page 25).
2. Click the **Broadband Status** option arrow in the upper right of the screen to display the Connection Status pop-up screen. (The following figure shows a static IP address configuration.)

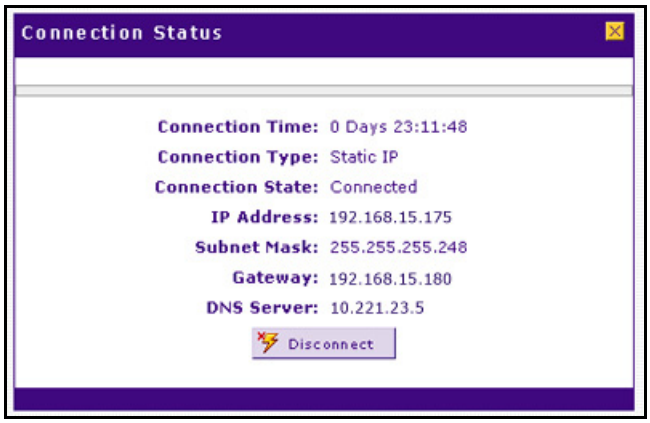


Figure 181.

The type of connection determines the information that is displayed on the Connection Status screen. The screen can display the information that is described in the following table:

Table 79. Connection Status screen information for an IPv4 connection

Item	Description
Connection Time	The period that the wireless VPN firewall has been connected through the WAN port.
Connection Type	The connection type can be either DHCP or Static IP.

Table 79. Connection Status screen information for an IPv4 connection (continued)

Item	Description
Connection Status	The connection status can be either Connected or Disconnected.
IP Address	The addresses that were automatically detected or that you configured on the Broadband ISP Settings (IPv4) screen. **Note:** For more information, see *Let the Wireless VPN Firewall Automatically Detect and Configure an IPv4 Internet Connection* on page 25 and *Manually Configure an IPv4 Internet Connection* on page 27.
Subnet Mask	
Gateway	
DNS Server	
DHCP Server	DHCP only. The DHCP server that was automatically detected. This field displays only if your ISP does not require a login and the IP address is acquired dynamically from your ISP. You have configured these ISP settings on the Broadband ISP Settings screen. **Note:** For more information, see *Let the Wireless VPN Firewall Automatically Detect and Configure an IPv4 Internet Connection* on page 25 and *Manually Configure an IPv4 Internet Connection* on page 27.
Lease Obtained	DHCP only. The time when the DHCP lease was obtained.
Lease Duration	DHCP only. The period that the DHCP lease remains in effect.

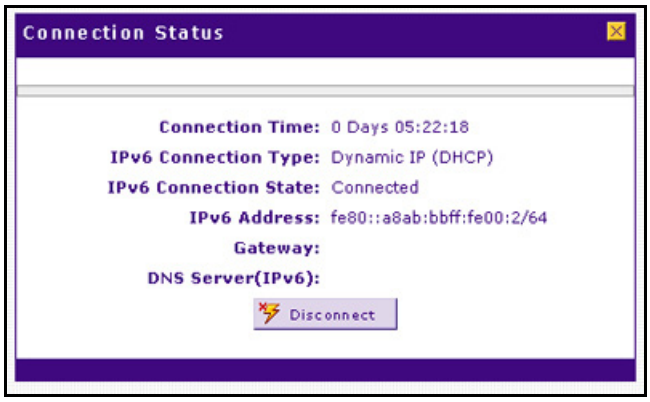
Depending on the type of connections, any of the following buttons might display on the Connection Status screen:

- **Renew**. Click to renew the DHCP lease.
- **Release**. Click to disconnect the DHCP connection.
- **Disconnect**. Click to disconnect the static IP connection.

IPv6 WAN Port Status

➢ **To view the IPv6 status of the WAN port:**

1. Select **Network Configuration > WAN Settings > Broadband ISP Settings (IPv6)**. The Broadband ISP Settings (IPv6) screen displays (see *Figure 15* on page 33).
2. Click the **Broadband Status (IPv6)** option arrow in the upper right of the screen to display the Connection Status pop-up screen. (The following figure shows a dynamic IP address configuration.)



The type of connection determines the information that is displayed on the Connection Status screen. The screen can display the information that is described in the following table:

Table 80. Connection Status screen information for an IPv6 connection

Item	Description
Connection Time	The period that the wireless VPN firewall has been connected through the WAN port.
IPv6 Connection Type	The connection type can be either Dynamic IP (DHCP) or Static.
IPv6 Connection Status	The connection status can be either Connected or Disconnected.
IP Address	The IPv6 addresses that were automatically detected or that you configured on the Broadband ISP Settings (IPv6) screen. **Note:** The Gateway and DNS Server (IPv6) fields apply only to a static IPv6 connection. **Note:** For more information, see *Let the Wireless VPN Firewall Automatically Configure an IPv6 Internet Connection* on page 33 and *Manually Configure an IPv6 Internet Connection* on page 34.
Gateway	
DNS Server (IPv6)	

Depending on the type of connections, any of the following buttons might display on the Connection Status screen:

- **Renew**. Click to renew the DHCP lease.
- **Release**. Click to disconnect the DHCP connection.
- **Disconnect**. Click to disconnect the static IP connection.

View the Attached Devices and the DHCP Log

The LAN Groups screen shows the network database, which is the Known PCs and Devices table, which contains all IP devices that wireless VPN firewall has discovered on the local network. The LAN Setup screen lets you access the DHCP log.

View the Attached Devices

➢ **To view the attached devices in the LAN Groups screen:**

Select **Network Configuration > LAN Settings > LAN Groups (IPv4)**. The LAN Groups (IPv4) screen displays. (The following figure shows some examples in the Known PCs and Devices table.)

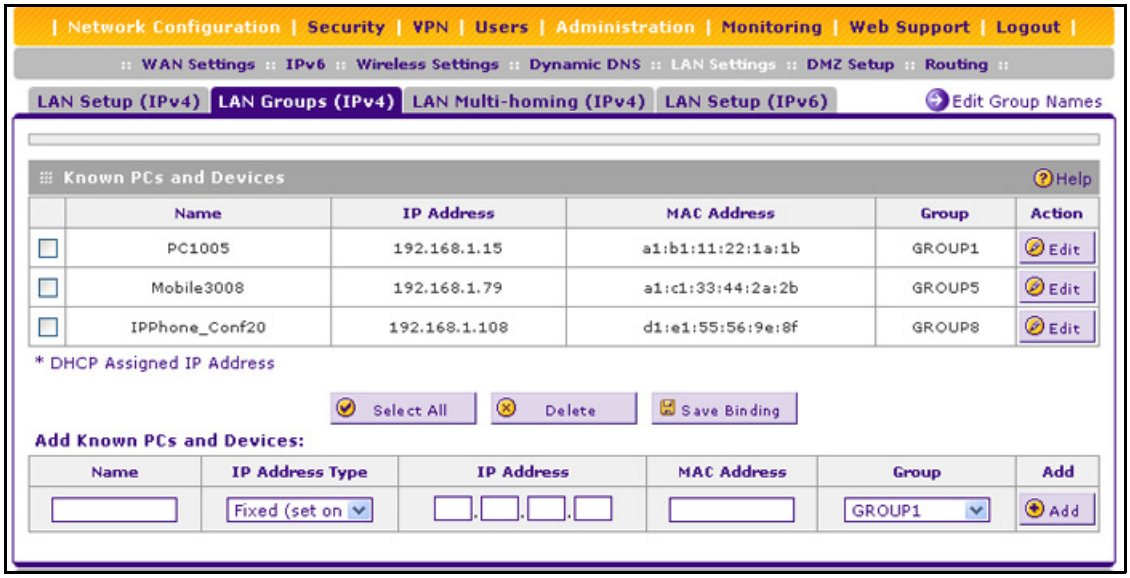

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
WAN Settings :: IPv6 :: Wireless Settings :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing
LAN Setup (IPv4) | LAN Groups (IPv4) | LAN Multi-homing (IPv4) | LAN Setup (IPv6)
Edit Group Names
Known PCs and Devices
Help
Name | IP Address | MAC Address | Group | Action
PC1005 | 192.168.1.15 | a1:b1:11:22:1a:1b | GROUP1 | Edit
Mobile3008 | 192.168.1.79 | a1:c1:33:44:2a:2b | GROUP5 | Edit
IPPhone_Conf20 | 192.168.1.108 | d1:e1:55:56:9e:8f | GROUP8 | Edit
* DHCP Assigned IP Address
Select All
Delete
Save Binding
Add Known PCs and Devices:
Name | IP Address Type | IP Address | MAC Address | Group | Add
Fixed (set on
GROUP1
Add

Figure 182.

The Known PCs and Devices table contains a list of all known PCs and network devices that are assigned dynamic IP addresses by the wireless VPN firewall, have been discovered by other means, or were manually added. Collectively, these entries make up the network database. For information about how to edit the Known PCs and Devices table or manually add entries to the table, see *Manage the Network Database* on page 60.

For each attached PC or device, the Known PCs and Devices table displays the following fields:

- **Check box**. Allows you to select the PC or device in the table.
- **Name**. The name of the PC or device. For computers that do not support the NetBIOS protocol, the name is displayed as *Unknown* (you can edit the entry manually to add a meaningful name). If the PC or device was assigned an IP address by the DHCP server, then the name is appended by an asterisk.
- **IP Address**. The current IP address of the PC or device. For DHCP clients of the wireless VPN firewall, this IP address does not change. If a PC or device is assigned a static IP address, you need to update this entry manually after the IP address on the PC or device has changed.
- **MAC Address**. The MAC address of the PC's or device's network interface.
- **Group**. Each PC or device can be assigned to a single LAN group. By default, a PC or device is assigned to Group 1. You can select a different LAN group from the Group

drop-down list in the Add Known PCs and Devices section or on the Edit Groups and Hosts screen.

- **Action**. The Edit table button, which provides access to the Edit Groups and Hosts screen.

Note: If the wireless VPN firewall is rebooted, the data in the Known PCs and Devices table is lost until the wireless VPN firewall rediscovers the devices.

View the DHCP Log

➢ **To review the most recent entries in the DHCP log:**

1. Select **Network Configuration > LAN Settings > LAN Setup (IPv4)**. The LAN Setup (IPv4) screen displays (see *Figure 27* on page 51).
2. Click the **DHCP Log** option arrow at the upper right of the LAN Setup (IPv4) screen. The DHCP Log displays in a pop-up screen:

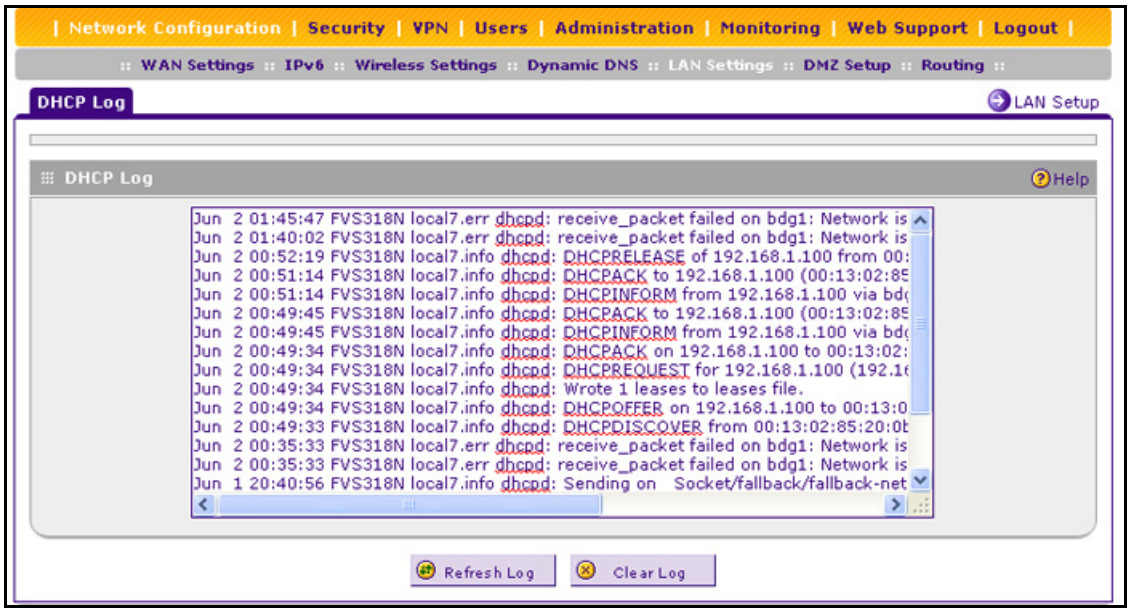

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
WAN Settings :: IPv6 :: Wireless Settings :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing
DHCP Log
LAN Setup
DHCP Log
Help
Jun 2 01:45:47 FVS318N local7.err dhcpd: receive_packet failed on bdg1: Network is
Jun 2 01:40:02 FVS318N local7.err dhcpd: receive_packet failed on bdg1: Network is
Jun 2 00:52:19 FVS318N local7.info dhcpd: DHCPRELEASE of 192.168.1.100 from 00:
Jun 2 00:51:14 FVS318N local7.info dhcpd: DHCPACK to 192.168.1.100 (00:13:02:85
Jun 2 00:51:14 FVS318N local7.info dhcpd: DHCPINFORM from 192.168.1.100 via bd
Jun 2 00:49:45 FVS318N local7.info dhcpd: DHCPACK to 192.168.1.100 (00:13:02:85
Jun 2 00:49:45 FVS318N local7.info dhcpd: DHCPINFORM from 192.168.1.100 via bd
Jun 2 00:49:34 FVS318N local7.info dhcpd: DHCPACK on 192.168.1.100 to 00:13:02:
Jun 2 00:49:34 FVS318N local7.info dhcpd: DHCPREQUEST for 192.168.1.100 (192.1
Jun 2 00:49:34 FVS318N local7.info dhcpd: Wrote 1 leases to leases file.
Jun 2 00:49:34 FVS318N local7.info dhcpd: DHCPOFFER on 192.168.1.100 to 00:13:0
Jun 2 00:49:33 FVS318N local7.info dhcpd: DHCPDISCOVER from 00:13:02:85:20:0
Jun 2 00:35:33 FVS318N local7.err dhcpd: receive_packet failed on bdg1: Network is
Jun 2 00:35:33 FVS318N local7.err dhcpd: receive_packet failed on bdg1: Network is
Jun 1 20:40:56 FVS318N local7.info dhcpd: Sending on Socket/fallback/fallback-net
Refresh Log
Clear Log

Figure 183.

To view the most recent entries, click **Refresh Log**. To delete all the existing log entries, click **Clear Log**. Click the **LAN Setup** option arrow in the upper right to display the LAN Setup (IPv4) screen, from which you can modify the DHCP settings (see *Configure a VLAN Profile* on page 51).

Diagnostics Utilities

The wireless VPN firewall provides diagnostic tools that help you analyze the status of the network and traffic conditions. Two types of tools are available:

- **Network diagnostic tools**. These tools include a ping utility, traceroute utility, and DNS lookup utility, and the option to display the routing tables.
- **Packet capture tool**. This tools lets you capture packets per interface in real time for a short period, and then download the packet information.

Note: For normal operation, diagnostic tools are not required.

➢ **To display the Diagnostics screen:**

Select **Monitoring > Diagnostics**.

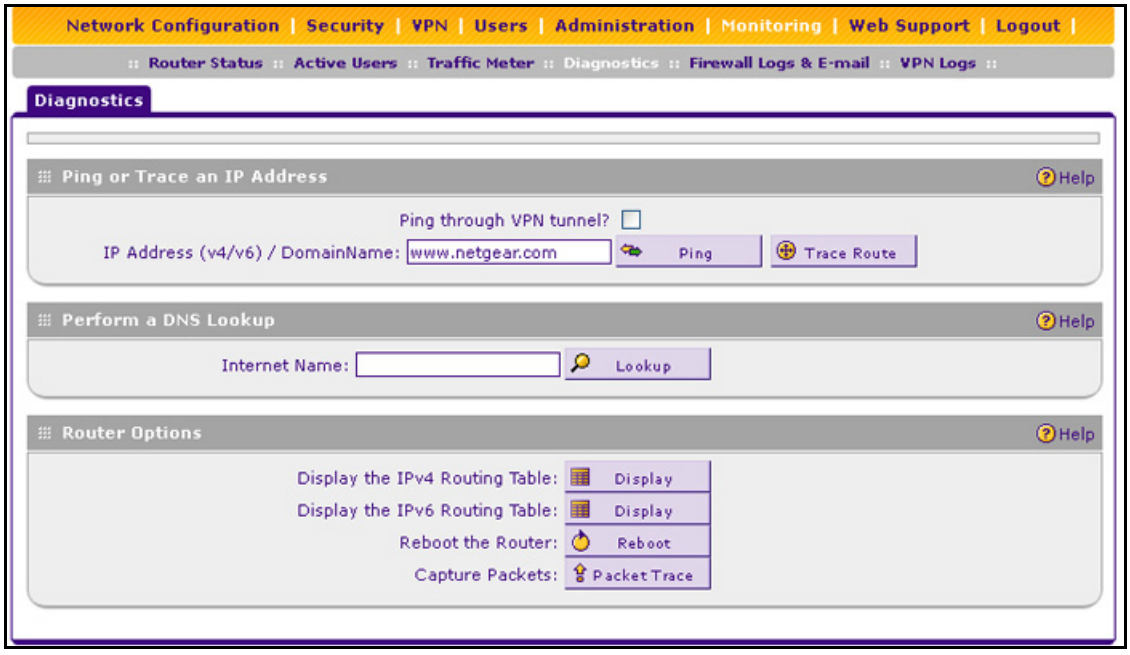


Figure 184.

Send a Ping Packet

Use the ping utility to send a ping packet request in order to check the connection between the wireless VPN firewall and a specific IP address or FQDN. If the request times out (no reply is received), it usually means that the destination is unreachable. However, some network devices can be configured not to respond to a ping. The ping results are displayed on a new screen.

➢ **To send a ping:**

1. In the Ping or Trace an IP Address section of the screen, in the IP Address (v4/v6) / DomainName field, enter the IPv4 or IPv6 address that you want to ping.
2. If the specified address is reached through a VPN tunnel, select the **Ping through VPN tunnel?** check box.
3. Click the **Ping** button. The results of the ping are displayed in a new screen. To return to the Diagnostics screen, click **Back** on the browser menu bar.

Trace a Route

A traceroute lists all routers between the source (the wireless VPN firewall) and the destination IP address.

➢ **To send a traceroute:**

1. In the Ping or Trace an IP Address section of the screen, in the IP Address (v4/v6) / DomainName field, enter the IPv4 or IPv6 address that you want to trace.
2. Click the **Traceroute** button. The results of the traceroute are displayed in a new screen. To return to the Diagnostics screen, click **Back** on the browser menu bar.

Look Up a DNS Address

A Domain Name Server (DNS) converts the Internet name (for example, www.netgear.com) to an IP address. If you need the IP address of a web, FTP, mail, or other server on the Internet, request a DNS lookup to find the IP address.

➢ **To look up a DNS address:**

1. In the Perform a DNS Lookup section of the screen, in the Internet Name field, enter a domain name.
2. Click the **Lookup** button. The results of the lookup action are displayed in a new screen. To return to the Diagnostics screen, click **Back** on the browser menu bar.

Display the Routing Tables

Displaying the internal routing table can assist NETGEAR technical support in diagnosing routing problems.

➢ **To display one of the routing tables:**

In Router Options section of the screen, do one of the following:

- Next to Display the IPv4 Routing Table, click the **Display** button.
- Next to Display the IPv6 Routing Table, click the **Display** button.

The routing table is shown in the Route Display screen that displays as a pop-up screen.

Capture Packets in Real Time

Capturing packets can assist NETGEAR technical support in diagnosing packet transfer problems. You can also use a traffic analyzer to do your own problem diagnoses.

➢ **To capture packets in real time:**

1. In Router Options section of the screen, next to Capture Packets, click the **Packet Trace** button. The Capture Packets pop-up screen displays.

Figure 185.

2. From the Select Network drop-down list, select the physical or virtual interface for which you want to capture packets.
3. Click **Start**. After a few seconds, the packet-tracing process starts, which is indicated by a message onscreen.
4. When you want to stop the packet-tracing process, click **Stop**. After a few seconds, the packet-tracing process stops, which is indicated by a message onscreen.
5. Click **Download**. Select a location to save the captured packets. (The default file name is pkt.cap.) The file is downloaded to the location that you specify.
6. When the download is complete, browse to the download location you specified, and verify that the file has been downloaded successfully.
7. Optional step: Send the file to NETGEAR technical support for analysis.

Reboot the Wireless VPN Firewall Remotely

You can perform a remote reboot, for example, when the wireless VPN firewall seems to have become unstable or is not operating normally.

Rebooting breaks any existing connections either to the wireless VPN firewall (such as your management session) or through the wireless VPN firewall (for example, LAN users accessing the Internet). However, connections to the Internet are automatically reestablished when possible.

➢ **To reboot the wireless VPN firewall:**

In Router Options section of the screen, next to Reboot the Router, click the **Reboot** button. The wireless VPN firewall reboots. The Diagnostics screen might remain visible during the reboot process, or a status message with a counter might show the number of seconds left until the reboot process is complete. The reboot process takes about 160 seconds.

11 Troubleshooting

This chapter provides troubleshooting tips and information for the wireless VPN firewall. After each problem description, instructions are provided to help you diagnose and solve the problem. For the common problems listed, go to the section indicated.

- Is the wireless VPN firewall on?

  Go to *Basic Functioning* on page 320.
- Have I connected the wireless VPN firewall correctly?

  Go to *Basic Functioning* on page 320.
- I cannot access the wireless VPN firewall's web management interface.

  Go to *Troubleshoot the Web Management Interface* on page 321.
- A time-out occurs.

  Go to *When You Enter a URL or IP Address, a Time-Out Error Occurs* on page 322.
- I cannot access the Internet or the LAN.

  Go to *Troubleshoot the ISP Connection* on page 323.
- I have problems with the IPv6 connection.

  Go to *Troubleshooting the IPv6 Connection* on page 324
- I have problems with the LAN connection.

  Go to *Troubleshoot a TCP/IP Network Using a Ping Utility* on page 327.
- I want to clear the configuration and start over again.

  Go to *Restore the Default Configuration and Password* on page 328.
- The date or time is not correct.

  Go to *Address Problems with Date and Time* on page 330.
- I need more information.

  Go to *Access the Knowledge Base and Documentation* on page 330.

Note: The wireless VPN firewall's diagnostic tools are explained in *Diagnostics Utilities* on page 316.

Basic Functioning

➢ **After you turn on power to the wireless VPN firewall, verify that the following sequence of events occurs:**

1. When power is first applied, verify that the Power LED is on.
2. After approximately 2 minutes, verify that:
   a. The Test LED is no longer lit.
   b. The left LAN port LEDs are lit for any local ports that are connected.
   c. The left WAN port LEDs are lit for any WAN ports that are connected.

   If a port's left LED is lit, a link has been established to the connected device. If a port is connected to a 1000 Mbps device, verify that the port's right LED is green. If the port functions at 100 Mbps, the right LED is amber. If the port functions at 10 Mbps, the right LED is off.

If any of these conditions do not occur, see the appropriate following section.

Power LED Not On

If the Power and other LEDs are off when your wireless VPN firewall is turned on, make sure that the power cord is correctly connected to your wireless VPN firewall and that the power supply adapter is correctly connected to a functioning power outlet.

If the error persists, you have a hardware problem and should contact NETGEAR technical support.

Test LED Never Turns Off

When the wireless VPN firewall is powered on, the Test LED turns on for approximately 2 minutes and then turns off when the wireless VPN firewall has completed its initialization. If the Test LED remains on, there is a fault within the wireless VPN firewall.

➢ **If all LEDs are still on more than several minutes minute after power-up, do the following:**

- Turn the power off, and then turn it on again to see if the wireless VPN firewall recovers.
- Reset the wireless VPN firewall's configuration to factory default settings. Doing so sets the wireless VPN firewall's IP address to **192.168.1.1**. This procedure is explained in *Restore the Default Configuration and Password* on page 328.

If the error persists, you might have a hardware problem and should contact NETGEAR technical support.

LAN or WAN Port LEDs Not On

- **If either the LAN LEDs or WAN LEDs do not light when the Ethernet connection is made, check the following:**
  - Make sure that the Ethernet cable connections are secure at the wireless VPN firewall and at the hub, router, or workstation.
  - Make sure that power is turned on to the connected hub, router, or workstation.
  - Be sure that you are using the correct cables:

    When connecting the wireless VPN firewall's WAN ports to one or two devices that provide the Internet connections, use the cables that are supplied with the devices. These cables could be standard straight-through Ethernet cables or Ethernet crossover cables.

Troubleshoot the Web Management Interface

- **If you cannot access the wireless VPN firewall's web management interface from a PC on your local network, check the following:**
  - Check the Ethernet connection between the PC and the wireless VPN firewall as described in the previous section (*LAN or WAN Port LEDs Not On*).
  - Make sure that your PC's IP address is on the same subnet as the wireless VPN firewall. If you are using the recommended addressing scheme, your PC's address should be in the range of 192.168.1.2 to 192.168.1.254.

    Note: If your PC's IP address is shown as 169.254.x.x: Windows and Mac operating systems generate and assign an IP address if the computer cannot reach a DHCP server. These autogenerated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the PC to the wireless VPN firewall and reboot your PC.

  - If your wireless VPN firewall's IP address has been changed and you do not know the current IP address, reset the wireless VPN firewall's configuration to factory default settings. This sets the wireless VPN firewall's IP address to **192.168.1.1**. This procedure is explained in *Restore the Default Configuration and Password* on page 328.

Tip: If you do not want to revert to the factory default settings and lose your configuration settings, you can reboot the wireless VPN firewall and use a sniffer to capture packets sent during the reboot. Look at the ARP packets to locate the wireless VPN firewall's LAN interface address.

- Make sure that you are using the SSL https://*address* login rather than the http://*address* login.
- Make sure that your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click **Refresh** to be sure that the Java applet is loaded.
- Try quitting the browser and launching it again.
- Make sure that you are using the correct login information. The factory default login name is admin, and the password is password. Make sure that Caps Lock is off when entering this information.

If the wireless VPN firewall does not save changes you have made in the web management Interface, check the following:

- When entering configuration settings, be sure to click the **Apply** button before moving to another menu or tab, or your changes are lost.
- Click the **Refresh** or **Reload** button in the web browser. The changes might have occurred, but the web browser might be caching the old configuration.

When You Enter a URL or IP Address, a Time-Out Error Occurs

➢ **A number of things could be causing this situation. Try the following troubleshooting steps:**

- Check whether other computers on the LAN work correctly. If they do, ensure that your computer's TCP/IP settings are correct. If you use a fixed (static) IP address, check the subnet mask, default gateway, DNS, and IP addresses on the Broadband ISP Settings screen. For more information, see *Manually Configure an IPv4 Internet Connection* on page 27.
- If the computer is configured correctly, but still not working, ensure that the wireless VPN firewall is connected and turned on. Connect to the web management interface, and check the wireless VPN firewall's settings. If you cannot connect to the wireless VPN firewall, see the information in the previous section (*Troubleshoot the Web Management Interface* on page 321).
- If the wireless VPN firewall is configured correctly, check your Internet connection (for example, your modem or router) to make sure that it is working correctly.

Troubleshoot the ISP Connection

If your wireless VPN firewall is unable to access the Internet, you should first determine whether the wireless VPN firewall is able to obtain a WAN IP address from the ISP. Unless you have been assigned a static IP address, your wireless VPN firewall requests an IP address from the ISP. You can determine whether the request was successful using the web management interface.

➢ **To check the WAN IP address:**

1. Launch your browser and navigate to an external site such as www.netgear.com.
2. Access the web management interface of the wireless VPN firewall's configuration at https://192.168.1.1.
3. Select **Network Configuration > WAN Settings**. The WAN Settings screen displays.
4. In the Action column for the interface for which you want to open the Connection Status screen, click the **Status** button. (For more information, see *View the WAN Port Status* on page 311.)
5. Check that an IP address is shown for the WAN port. If 0.0.0.0 is shown, your wireless VPN firewall has not obtained an IP address from your ISP.

➢ **If your wireless VPN firewall is unable to obtain an IP address from the ISP, you might need to force your modem or router to recognize your new wireless VPN firewall by performing the following procedure:**

1. Turn off the power to the modem or router.
2. Turn off the power to your wireless VPN firewall.
3. Wait 5 minutes, and then turn on the power to the modem or router.
4. When the modem's or router's LEDs indicate that it has reacquired synchronization with the ISP, turn on the power to your wireless VPN firewall.

If your wireless VPN firewall is still unable to obtain an IP address from the ISP, the problem might be one of the following:

- Your ISP might require a login program.
  Ask your ISP whether they require PPP over Ethernet (PPPoE) or some other type of login.
- If your ISP requires a login, you might have incorrectly set the login name and password.
- For IPv4 connections, your ISP might check for your PC's host name.
  On the Broadband ISP Settings (IPv4) screen, in the Account Name field, enter the host name, system name, or account name that was assigned to you by your ISP. You might also have to enter the assigned domain name or workgroup name in the Domain Name field, and you might have to enter additional information. For more information, see *Manually Configure an IPv4 Internet Connection* on page 27.

- Your ISP allows only one Ethernet MAC address to connect to the Internet, and might check for your PC's MAC address. In this case, do one of the following:
  - Inform your ISP that you have bought a new network device, and ask them to use the wireless VPN firewall's MAC address.
  - Configure your wireless VPN firewall to spoof your PC's MAC address. You can do this in the Router's MAC Address section on the WAN Advanced Options screen. For more information, see *Configure Advanced WAN Options and Other Tasks* on page 43.

If your wireless VPN firewall can obtain an IP address, but an attached PC is unable to load any web pages from the Internet:

- Your PC might not recognize any DNS server addresses.

  A DNS server is a host on the Internet that translates Internet names (such as www.netgear.com) to numeric IP addresses. Typically your ISP provides the addresses of one or two DNS servers for your use. You can configure your PC manually with DNS addresses, as explained in your operating system documentation.

- Your PC might not have the wireless VPN firewall configured as its TCP/IP gateway.

Troubleshooting the IPv6 Connection

If you have difficulty connecting over an IPv6 section, there might be an incorrect configuration on the wireless VPN firewall or the computer from which you are trying to connect to the wireless VPN firewall:

Check the wireless VPN firewall:

- By default, the wireless VPN firewall is set to IPv4-only mode. Make sure that the wireless VPN firewall is set to IPv4/IPv6 mode (see *Configure the IPv6 Routing Mode* on page 36).
- Make sure that the ISP settings are correct (see *Manually Configure an IPv6 Internet Connection* on page 34). The wireless VPN firewall cannot receive a valid IPv6 address if the Internet connection is not correctly configured.
- Make sure that the wireless VPN firewall can provide IPv6 addresses to the computers on the LAN (see *Configure IPv6 LAN Settings* on page 64). Check the settings on the LAN Setup (IPv6) screen, and if applicable for your type of configuration, on the RADVD screen.

Check the computer:

- Make sure that the operating system supports IPv6. Normally, the following operating systems support IPv6:
  - Windows 7, all 32- and 64-bit versions
  - Windows Vista, all 32- and 64-bit versions
  - Windows XP Professional SP3 (32- and 64-bit)
  - Windows Server 2008, all versions
  - Windows Server 2008 R2, all versions

- Windows Server 2003, all versions
- Windows server 2003 R2, all versions
- Linux and other UNIX-based systems with a correctly configured kernel
- MAC OS X

- Make sure that IPv6 is enabled on the computer. On a computer that runs a Windows-based operating system, do the following (note that the steps might differ on the various Windows operating systems):

  a. Open the Network Connections screen or the Network and Sharing Center screen. For example, on the Windows taskbar, click **Start**, then select **Control Panel**, and then **Network Connections**.

  b. Click or double-click **Local Area Connection** for the connection to the wireless VPN firewall. The Local Area Connection Properties screen displays:

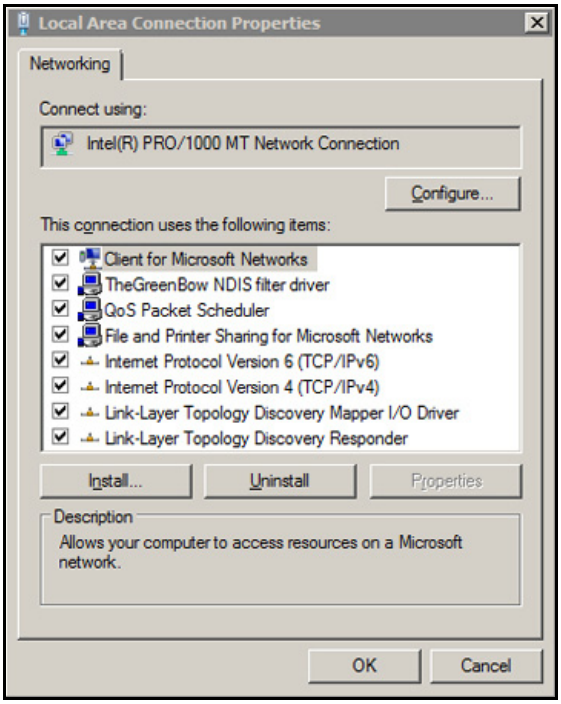


Figure 186.

  c. Make sure that Internet Protocol Version 6 (TCP/IPv6) displays, as is shown on the previous screen.

- Make sure that the computer has an IPv6 address. If the computer has a link-local address only, it cannot reach the wireless VPN firewall or the Internet. On a computer that runs a Windows-based operating system, do the following (note that the steps might differ on the various Windows operating systems):

  a. Open the Network Connections screen or the Network and Sharing Center screen. For example, on the Windows taskbar, click **Start**, then select **Control Panel**, and then **Network Connections**.

  b. Click or double-click **Local Area Connection** for the connection to the wireless VPN firewall.

c. Click or double-click **View status of this connection**. The Local Area Connection Status screen displays:

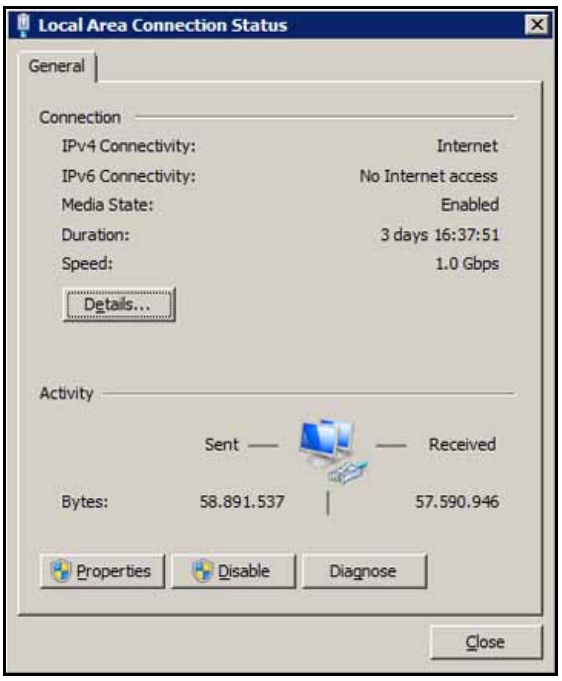


Figure 187.

d. Make sure that Internet access shows for the IPv6 connection. (The previous screen shows that there is no Internet access.)

e. Click **Details**. The Network Connection Details screen displays.

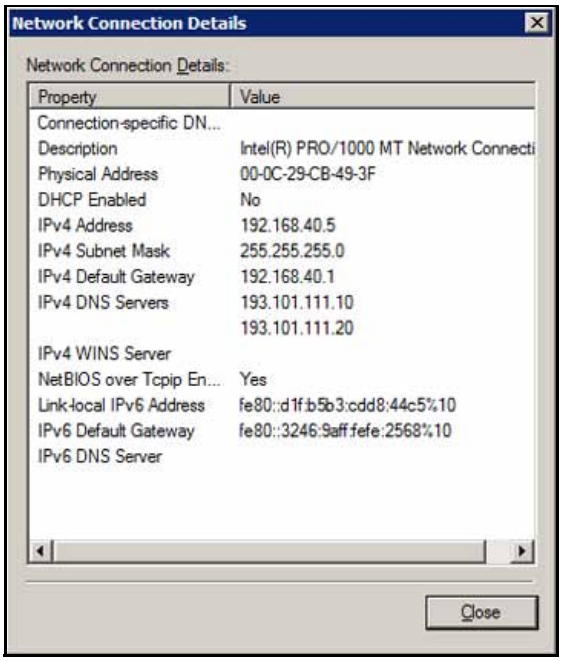


Figure 188.

f. Make sure that an IPv6 address shows. The previous screen does not show an IPv6 address for the computer but only a link-local IPv6 address and an IPv6 default gateway address, both of which start with FE80.

Troubleshoot a TCP/IP Network Using a Ping Utility

Most TCP/IP terminal devices and firewalls contain a ping utility that sends an echo request packet to the designated device. The device then responds with an echo reply. You can easily troubleshoot a TCP/IP network by using the ping utility in your PC or workstation.

Test the LAN Path to Your Wireless VPN Firewall

You can ping the wireless VPN firewall from your PC to verify that the LAN path to the wireless VPN firewall is set up correctly.

➢ **To ping the wireless VPN firewall from a PC running Windows 95 or later:**

1. From the Windows taskbar, click **Start** and select **Run**.
2. In the field provided, type **ping** followed by the IP address of the wireless VPN firewall, for example:

   ping 192.168.1.1

3. Click **OK**. A message similar to the following should display:

   ```
   Pinging <IP address> with 32 bytes of data
   ```

   If the path is working, you will see this message:

   ```
   Reply from <IP address>: bytes=32 time=NN ms TTL=xxx
   ```

   If the path is not working, you will see this message:

   ```
   Request timed out
   ```

   If the path is not functioning correctly, you could have one of the following problems:

   - Wrong physical connections
     - Make sure that the LAN port LED is on. If the LED is off, follow the instructions in *LAN or WAN Port LEDs Not On* on page 321.
     - Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and wireless VPN firewall.
   - Wrong network configuration
     - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your PC or workstation.
     - Verify that the IP address for your wireless VPN firewall and your workstation are correct and that the addresses are on the same subnet.

Test the Path from Your PC to a Remote Device

After verifying that the LAN path works correctly, test the path from your PC to a remote device. From the Windows Run dialog box, type:

ping -n 10 <IP address>

in which `<IP address>` is the IP address of a remote device such as your ISP's DNS server.

If the path is functioning correctly, replies as in the previous section are displayed. If you do not receive replies:

- Check that your PC has the IP address of your wireless VPN firewall listed as the default gateway. If the IP configuration of your PC is assigned by DHCP, this information is not visible in your PC's Network Control Panel.
- Check to see that the network address of your PC (the portion of the IP address that is specified by the netmask) is different from the network address of the remote device.
- Check that the modem or router is connected and functioning.
- For IPv4 connections, if your ISP assigned a host name, system name, or account name to your PC, enter that name in the Account Name field on the Broadband ISP Settings (IPv4) screen. You might also have to enter the assigned domain name or workgroup name in the Domain Name field, and you might have to enter additional information. For more information, see *Manually Configure an IPv4 Internet Connection* on page 27.
- Your ISP could be rejecting the Ethernet MAC addresses of all but one of your PCs. Many broadband ISPs restrict access by allowing traffic only from the MAC address of your broadband modem, but some ISPs additionally restrict access to the MAC address of a single PC connected to that modem. If this is the case, you need to configure your wireless VPN firewall to *clone* or *spoof* the MAC address from the authorized PC. You can do this in the Router's MAC Address section on the WAN Advanced Options screen. For more information, see *Configure Advanced WAN Options and Other Tasks* on page 43.

Restore the Default Configuration and Password

➢ **To reset the wireless VPN firewall to the original factory default settings, you can use one of the following two methods:**

- Press the factory default **Reset** button on the rear panel of the wireless VPN firewall (see *Rear Panel* on page 17) and hold the button for about 8 seconds until the Test LED turns on and begins to blink (about 30 seconds). To restore the factory default settings when you do not know the administration password or IP address, you need to use the factory default Reset button method.
- Use the Default button on the Settings Backup and Firmware Upgrade screen:

  a. Select **Administration > Settings Backup and Firmware Upgrade**:

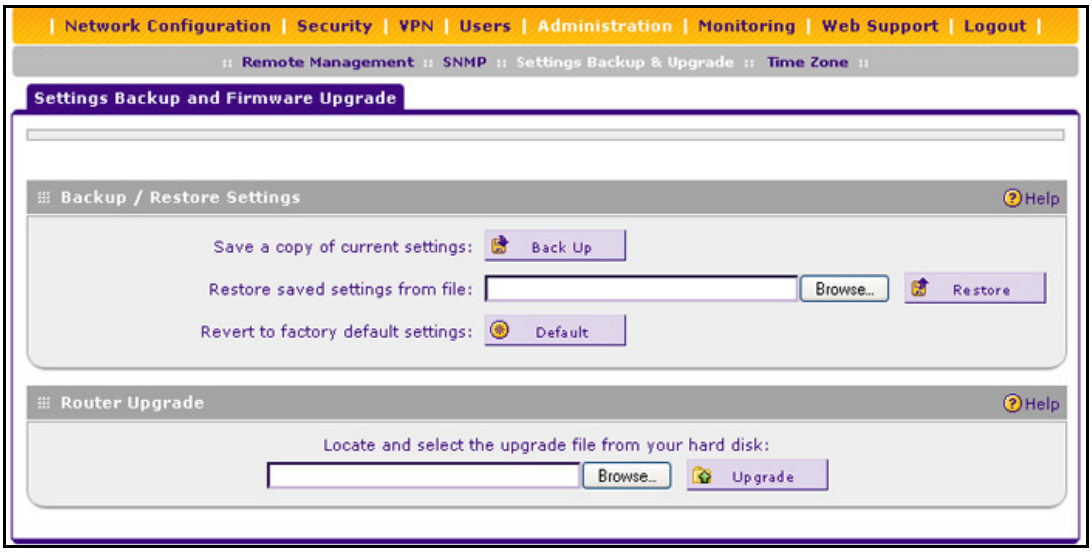

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
Remote Management :: SNMP :: Settings Backup & Upgrade :: Time Zone
Settings Backup and Firmware Upgrade
Backup / Restore Settings
Help
Save a copy of current settings:
Back Up
Restore saved settings from file:
Browse...
Restore
Revert to factory default settings:
Default
Router Upgrade
Help
Locate and select the upgrade file from your hard disk:
Browse...
Upgrade

Figure 189.

b. Click the **Default** button.

The wireless VPN firewall reboots. During the reboot process, the Settings Backup and Firmware Upgrade screen might remain visible, or a status message with a counter might show the number of seconds left until the reboot process is complete. The reboot process takes about 160 seconds. (If you can see the unit: The reboot process is complete when the Test LED on the front panel goes off.)

WARNING!

When you press the hardware factory default Reset button or click the software Default button, the wireless VPN firewall settings are erased. All firewall rules, VPN policies, LAN and WAN settings, and other settings are lost. Back up your settings if you intend on using them.

Note: After rebooting with factory default settings, the wireless VPN firewall's password is **password**, and the LAN IP address is **192.168.1.1**.

Address Problems with Date and Time

The System Date & Time screen displays the current date and time of day (see *Configure Date and Time Service* on page 288). The wireless VPN firewall uses the Network Time Protocol (NTP) to obtain the current time from one of several network time servers on the Internet. Each entry in the log is stamped with the date and time of day.

Problems with the date and time function can include:

- Date shown is January 1, 2000. Cause: The wireless VPN firewall has not yet successfully reached a network time server. Check that your Internet access settings are configured correctly. If you have just completed configuring the wireless VPN firewall, wait at least 5 minutes, and check the date and time again.
- Time is off by 1 hour. Cause: The wireless VPN firewall does not automatically sense daylight savings time. Go to the Time Zone screen, and select or clear the **Automatically Adjust for Daylight Savings Time** check box.

Access the Knowledge Base and Documentation

➢ **To access NETGEAR's knowledge base for the wireless VPN firewall:**

Select **Support > Knowledge Base**.

➢ **To access NETGEAR's documentation library for your wireless VPN firewall model:**

Select **Support > Documentation**.

Default Settings and Technical Specifications

A

This appendix provides the default settings and the physical and technical specifications of the wireless VPN firewall in the following sections:

- *Default Settings*
- *Physical and Technical Specifications*

Default Settings

You can use the factory default **Reset** button located on the rear panel to reset all settings to their factory defaults. This is called a hard reset (for more information, see *Revert to Factory Default Settings* on page 286):

- To perform a hard reset, press and hold the factory default Reset button for approximately 8 seconds (until the Test LED blinks rapidly). The wireless VPN firewall returns to the factory configuration settings that are shown in the following table.
- Pressing the factory default Reset button for a shorter period of time simply causes the wireless VPN firewall to reboot.

The following table shows the default configuration settings for the wireless VPN firewall:

Table 81. Wireless VPN firewall factory default configuration settings

Feature		Default behavior
Router login		
	User login URL	https://192.168.1.1
	Administrator user name (case-sensitive)	admin
	Administrator login password (case-sensitive)	password
	Guest user name (case-sensitive)	guest
	Guest login password (case-sensitive)	password

Table 81. Wireless VPN firewall factory default configuration settings (continued)

Feature		Default behavior
Internet connection		
	WAN MAC address	Use default address
	WAN MTU size	1500
	Port speed	AutoSense
Local area network (LAN)		
	LAN IPv4 address	192.168.1.1
	Subnet mask	255.255.255.0
	RIP direction	None
	RIP version	Disabled
	RIP authentication	Disabled
	DHCP server	Enabled
	DHCP starting IPv4 address	192.168.1.2
	DHCP ending IPv4 address	192.168.1.100
	DMZ	Disabled
Management		
	Time zone	GMT
	Time zone adjusted for daylight savings time	Disabled
	SNMP	Disabled
	Remote management	Disabled
Firewall		
	Inbound (communications coming in from the Internet)	All communication denied (except traffic on port 80, the HTTP port)
	Outbound (communications from the LAN to the Internet)	All communication allowed
	Source MAC filtering	Disabled
	Stealth mode	Enabled
	Respond to ping on Internet ports	Disabled

Table 81. Wireless VPN firewall factory default configuration settings (continued)

Feature		Default behavior
Wireless radio and access point		
	Wireless radio	Enabled
	Default virtual access point	ap1
	Default network name (SSID)	FVS318N_1
	Broadcast SSID	Enabled
	Default security profile	default1
	Security	Open, no encryption
	Transmission rate	Best[1]
	Country and region	Unites States
	802.11 wireless mode	802.11ng
	80211b/g/n radio frequency channel	Auto
	80211n channel spacing	20 MHz
	80211n control side band	Lower

1. The maximum wireless signal rate derived from IEEE Standard 802.11 specifications. The actual throughput varies. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate.

Physical and Technical Specifications

The following table shows the physical and technical specifications for the wireless VPN firewall:

Table 82. Wireless VPN firewall physical and technical specifications

Feature		Specification
Network protocol and standards compatibility		
	Data and Routing Protocols	TCP/IP, RIP-1, RIP-2, PPP over Ethernet (PPPoE), DHCP, DHCPv6
Power plug (localized to the country of sale)		
	North America	120V, 60 Hz, input
	United Kingdom, Australia	240V, 50 Hz, input
	Europe	230V, 50 Hz, input
	Input, for all regions	12VDC @ 1A output

Table 82. Wireless VPN firewall physical and technical specifications (continued)

Feature		Specification
Dimensions and weight		
	Dimensions (W x H x D)	19 x 12.5 x 3.5 cm (7.5 X 4.9 X 1.4 in)
	Weight	0.59 kg (1.3 lb)
Environmental specifications		
	Operating temperatures	0º to 40ºC
		32º to 104ºF
	Storage temperatures	–20º to 70ºC
		–4º to 158ºF
	Operating humidity	90% maximum relative humidity, noncondensing
	Storage humidity	95% maximum relative humidity, noncondensing
Electromagnetic emissions		
	Meets requirements of	FCC Part 15 Class B
		VCCI Class B
		EN 55 022 (CISPR 22), Class B
Wireless compliance		
	See *Appendix D, Notification of Compliance (Wireless)*.	
Interface specifications		
	LAN	8 LAN autosensing 10/100/1000BASE-T, RJ-45, one of which is a configurable DMZ interface
	WAN	1 WAN autosensing 10/100/1000BASE-T, RJ-45
	1 administrative console port	RS-232

The following table shows the IPSec VPN specifications for the wireless VPN firewall:

Table 83. Wireless VPN firewall IPSec VPN specifications

Setting	Specification
Network Management	Web-based configuration and status monitoring
Number of concurrent users supported	5
IPSec authentication algorithm	SHA-1, MD5
IPSec encryption algorithm	DES, 3DES, AES-128, AES-192, AES-256
IPSec key exchange	IKE, manual key, pre-shared key, PKI, X.500

Table 83. Wireless VPN firewall IPSec VPN specifications (continued)

Setting	Specification
IPSec authentication types	Local user database, RADIUS PAP, RADIUS CHAP
IPSec certificates supported	CA certificates, self-signed certificate

The following table shows the SSL VPN specifications for the wireless VPN firewall:

Table 84. Wireless VPN firewall SSL VPN specifications

Setting	Specification
Network Management	Web-based configuration and status monitoring
Number of concurrent users supported	2
SSL versions	SSLv3, TLS1.0
SSL encryption algorithm	DES, 3DES, ARC4, AES-128, AES-192, AES-256
SSL message integrity	MD5, SHA-1, MAC-MD5/SHA-1, HMAC-MD5/SHA-1
SSL authentication types	Local user database, RADIUS-PAP, RADIUS-CHAP, RADIUS-MSCHAP, RADIUS-MSCHAPv2, WiKID-PAP, WiKID-CHAP, MIAS-PAP, MIAS-CHAP, NT domain, Active Directory, LDAP
SSL certificates supported	CA certificates, self-signed certificate

The following table shows the wireless specifications for the wireless VPN firewall:

Table 85. Wireless VPN firewall wireless specifications

Setting	Specification
802.11bg data rates	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps, and auto-rate capable
802.11ng/n data rates	Data rates for a channel width of 20 MHz and a (short) guard interval of 400 ms: Best (automatic), 7.2 Mbps, 14.4 Mbps, 21.7 Mbps, 28.9 Mbps, 43.3 Mbps, 57.8 Mbps, 65 Mbps, 72.2 Mbps, 14.44 Mbps, 28.88 Mbps, 43.33 Mbps, 57.77 Mbps, 86.66 Mbps, 115.56 Mbps, 130 Mbps, 144.44 Mbps
	Data rates for a channel width of 40 MHz and a (short) guard interval of 400 ms: Best (automatic), 15 Mbps, 30 Mbps, 45 Mbps, 60 Mbps, 90 Mbps, 120 Mbps, 135 Mbps, 150 Mbps, 30 Mbps, 60 Mbps, 90 Mbps, 120 Mbps, 180 Mbps, 240 Mbps, 270 Mbps, 300 Mbps
802.11b/bg/ng/n operating frequencies	• 2.412–2.462 GHz (US) • 2.457–2.462 GHz (Spain) • 2.457–2.472 GHz (France) • 2.412–2.472 GHz (Europe ETSI)
802.11 b/bg/ng/n encryption	64-bits and 128-bits WEP, TKIP, CCMP data encryption
Network management	Web-based configuration and status monitoring

Two-Factor Authentication

B

This appendix provides an overview of two-factor authentication, and an example of how to implement the WiKID solution. This appendix contains the following sections:

- *Why Do I Need Two-Factor Authentication?*
- *NETGEAR Two-Factor Authentication Solutions*

Why Do I Need Two-Factor Authentication?

In today's market, online identity theft and online fraud continue to be one of the fast-growing cybercrime activities used by many unethical hackers and cybercriminals to steal digital assets for financial gains. Many companies and corporations are losing millions of dollars and running into risks of revealing their trade secrets and other proprietary information as a result of these cybercrime activities. Security threats and hackers have become more sophisticated, and user names, encrypted passwords, and the presence of firewalls are no longer enough to protect the networks from being compromised. IT professionals and security experts have recognized the need to go beyond the traditional authentication process by introducing and requiring additional factors in the authentication process. NETGEAR has also recognized the need to provide more than just a firewall to protect the networks. NETGEAR has implemented a more robust authentication system known as two-factor authentication (2FA or T-FA) to help address the fast-growing network security issues.

What Are the Benefits of Two-Factor Authentication?

- **Stronger security**. Passwords cannot efficiently protect the corporate networks because attackers can easily guess simple passwords or users cannot remember complex and unique passwords. One-time passcode (OTP) strengthens and replaces the need to remember complex password.
- **No need to replace existing hardware**. Two-factor authentication can be added to existing NETGEAR products through a firmware upgrade.
- **Quick to deploy and manage**. The WiKID solution integrates seamlessly with the NETGEAR SSL and VPN firewall products.
- **Proven regulatory compliance**. Two-factor authentication has been used as a mandatory authentication process for many corporations and enterprises worldwide.

What Is Two-Factor Authentication?

Two-factor authentication is a security solution that enhances and strengthens security by implementing multiple factors of the authentication process that challenge and confirm the users' identities before they can gain access to the network. There are several factors that are used to validate the users to make sure that you are who you say you are. These factors are:

- Something you know—for example, your password or your PIN.
- Something you have—for example, a token with generated passcode that is 6 to 8 digits in length.
- Something you are—for example, biometrics such as fingerprints or retinal prints.

This appendix focuses on and discusses only the first two factors, something you know and something you have. This security method can be viewed as a two-tiered authentication approach because it typically relies on what you know and what you have. A common example of two-factor authentication is a bank (ATM) card that has been issued by a bank institute:

- The PIN to access your account is *something you know.*
- The ATM card is *something you have.*

You need to have both of these factors to gain access to your bank account. Similar to the way ATM cards work, access to the corporate networks and data can also be strengthened using a combination of multiple factors such as a PIN and a token (hardware or software) to validate the users and reduce the incidence of online identity theft.

NETGEAR Two-Factor Authentication Solutions

NETGEAR has implemented 2 two-factor authentication solutions from WiKID. WiKID is the software-based token solution. So instead of using only Windows Active Directory or LDAP as the authentication server, administrators now have the option to use WiKID to perform two-factor authentication on NETGEAR SSL and VPN firewall products.

The WiKID solution is based on a request-response architecture where a one-time passcode (OTP), which is time-synchronized with the authentication server, is generated and sent to the user after the validity of a user credential has been confirmed by the server.

The request-response architecture is capable of self-service initialization by end users, dramatically reducing implementation and maintenance costs.

Here is an example of how WiKID works:

➢ **To use WiKID (for end users):**

1. Launch the WiKID token software, enter the PIN that has been provided (*something the user know*s), and then click **Continue** to receive the OTP from the WiKID authentication server:

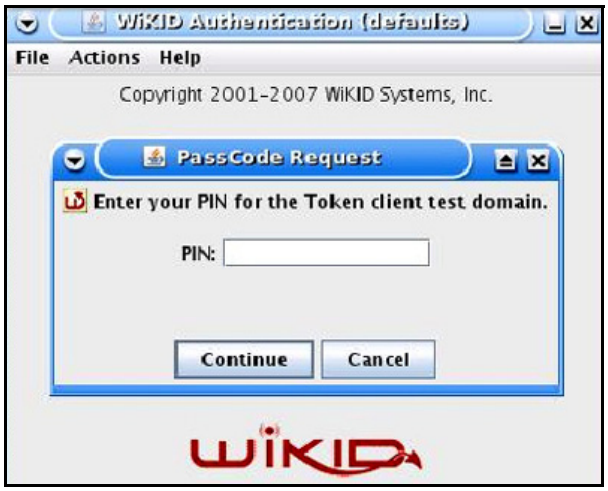


Figure 190.

2. A one-time passcode (*something the user has*) is generated.

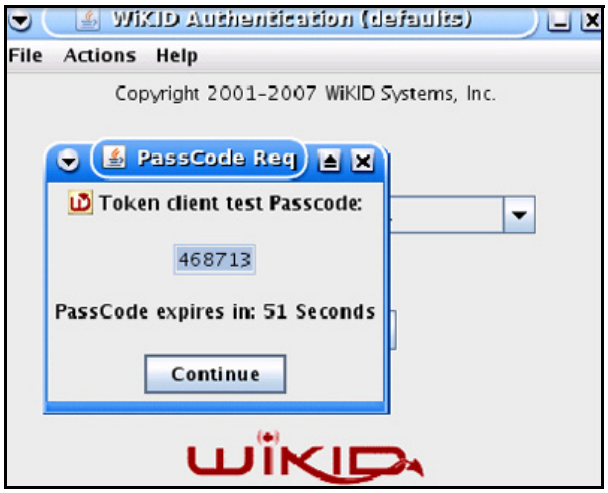


Figure 191.

Note: The one-time passcode is time-synchronized to the authentication server so that the OTP can be used only once and needs to be used before the expiration time. If a user does not use this passcode before it expires, the user needs to go through the request process again to generate a new OTP.

3. Proceed to the 2 Factor Authentication login screen, and enter the one-time passcode as the login password.

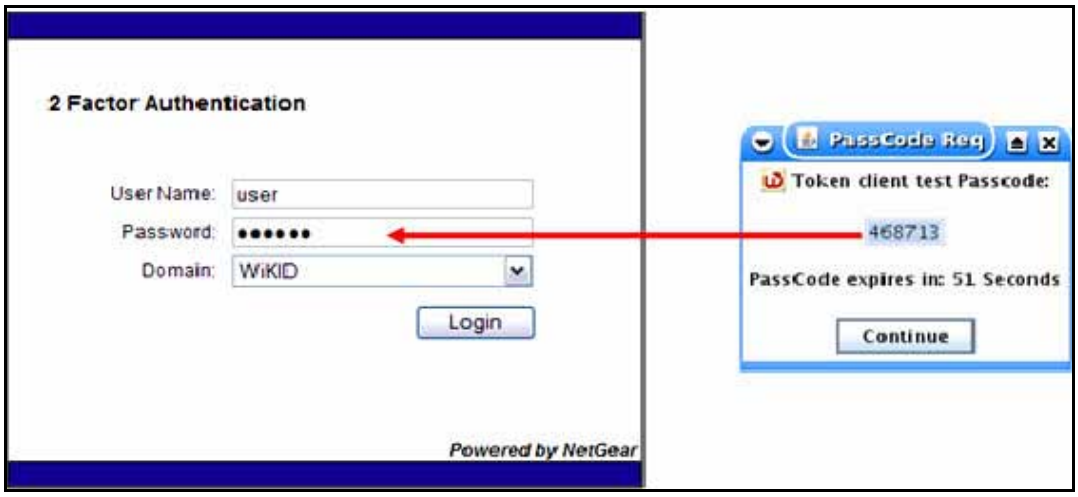

2 Factor Authentication
User Name:
user
Password:
Domain:
WiKID
Login
Powered by NetGear
PassCode Req
Token client test Passcode:
468713
PassCode expires in: 51 Seconds
Continue

Figure 192.

Notification of Compliance (Wired)

C

NETGEAR Wired Products

Regulatory Compliance Information

This section includes user requirements for operating this product in accordance with National laws for usage of radio spectrum and operation of radio devices. Failure of the end-user to comply with the applicable requirements may result in unlawful operation and adverse action against the end-user by the applicable National regulatory authority.

This product's firmware limits operation to only the channels allowed in a particular Region or Country. Therefore, all options described in this user's guide may not be available in your version of the product.

FCC Requirements for Operation in the United States

FCC Information to User

This product does not contain any user serviceable components and is to be used with approved antennas only. Any product changes or modifications will invalidate all applicable regulatory certifications and approvals

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Guidelines for Human Exposure

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 20 cm between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Declaration Of Conformity

We, NETGEAR, Inc., 350 East Plumeria Drive, San Jose, CA 95134, declare under our sole responsibility that the ProSafe Wireless-N 8-Port Gigabit VPN Firewall FVS318N complies with Part 15 of FCC Rules.

Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

FCC Radio Frequency Interference Warnings & Instructions

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following methods:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an electrical outlet on a circuit different from that which the radio receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications made to the product, unless expressly approved by NETGEAR, Inc., could void the user's right to operate the equipment.

Canadian Department of Communications Radio Interference Regulations

This digital apparatus, ProSafe Wireless-N 8-Port Gigabit VPN Firewall FVS318N, does not exceed the Class B limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

This Class [B] digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe [B] est conforme à la norme NMB-003 du Canada.

European Union

The ProSafe Wireless-N 8-Port Gigabit VPN Firewall FVS318N complies with essential requirements of EU EMC Directive 2004/108/EC and Low Voltage Directive 2006/95/EC as supported by applying the following test methods and standards:

- EN55022: 2006 / A1: 2007
- EN55024: 1998 / A1: 2001 / A2 : 2003
- EN60950-1: 2005 2nd Edition
- EN 61000-3-2:2006
- EN 61000-3-3:1995 w/A1: 2001+A2: 2005

GPL License Agreement

GPL may be included in this product; to view the GPL license agreement go to *ftp://downloads.netgear.com/files/GPLnotice.pdf*.

For GNU General Public License (GPL) related information, please visit *http://support.netgear.com/app/answers/detail/a_id/2649*.

Additional Copyrights

AES	Copyright (c) 2001, Dr. Brian Gladman, brg@gladman.uk.net, Worcester, UK. All rights reserved. TERMS Redistribution and use in source and binary forms, with or without modification, are permitted subject to the following conditions: 1. Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. The copyright holder's name must not be used to endorse or promote any products derived from this software without his specific prior written permission. This software is provided "as is" with no express or implied warranties of correctness or fitness for purpose.
Open SSL	Copyright (c) 1998–2000 The OpenSSL Project. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (*http://www.openssl.org/*). 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, contact openssl-core@openssl.org. 5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project. 6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (*http://www.openssl.org/*). THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS," AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

MD5	Copyright (C) 1990, RSA Data Security, Inc. All rights reserved. License to copy and use this software is granted provided that it is identified as the “RSA Data Security, Inc. MD5 Message-Digest Algorithm” in all material mentioning or referencing this software or this function. License is also granted to make and use derivative works provided that such works are identified as “derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm” in all material mentioning or referencing the derived work. RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided “as is” without express or implied warranty of any kind. These notices must be retained in any copies of any part of this documentation and/or software.
PPP	Copyright (c) 1989 Carnegie Mellon University. All rights reserved. Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by Carnegie Mellon University. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.
Zlib	zlib.h. Interface of the zlib general purpose compression library version 1.1.4, March 11th, 2002. Copyright (C) 1995–2002 Jean-loup Gailly and Mark Adler. This software is provided “as is,” without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software. Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions: 1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required. 2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software. 3. This notice may not be removed or altered from any source distribution. Jean-loup Gailly: jloup@gzip.org; Mark Adler: madler@alumni.caltech.edu. The data format used by the zlib library is described by RFCs (Request for Comments) 1950 to 1952 in the files rfc1950.txt (zlib format), rfc1951.txt (deflate format), and rfc1952.txt (gzip format). For more information, see *http://www.ietf.org/rfc/*.

Notification of Compliance (Wireless)

D

NETGEAR Wireless Routers, Gateways, APs

Regulatory Compliance Information

Note: This section includes user requirements for operating this product in accordance with National laws for usage of radio spectrum and operation of radio devices. Failure of the end-user to comply with the applicable requirements may result in unlawful operation and adverse action against the end-user by the applicable National regulatory authority.

Note: This product's firmware limits operation to only the channels allowed in a particular Region or Country. Therefore, all options described in this user's guide may not be available in your version of the product.

Europe – EU Declaration of Conformity

Marking by the above symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC). This equipment meets the following conformance standards:

EN300 328 (2.4Ghz), EN301 489-17 EN60950-1

For complete DoC, visit the NETGEAR EU Declarations of Conformity website at:
http://support.netgear.com/app/answers/detail/a_id/11621/.

EDOC in Languages of the European Community

Language	Statement
Cesky [Czech]	*NETGEAR* Inc. tímto prohlašuje, že tento Radiolan je ve shode se základními požadavky a dalšími príslušnými ustanoveními smernice 1999/5/ES.
Dansk [Danish]	Undertegnede *NETGEAR Inc.* erklærer herved, at følgende udstyr Radiolan overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklärt *NETGEAR Inc.*, dass sich das Gerät Radiolan in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab *NETGEAR Inc.* seadme Radiolan vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, *NETGEAR Inc.*, declares that this Radiolan is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

Español [Spanish]	Por medio de la presente *NETGEAR Inc.* declara que el Radiolan cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ *NETGEAR Inc.* ΔΗΛΩΝΕΙ ΟΤΙ Radiolan ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Français [French]	Par la présente *NETGEAR Inc.* déclare que l'appareil Radiolan est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Italiano [Italian]	Con la presente *NETGEAR Inc.* dichiara che questo Radiolan è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo *NETGEAR Inc.* deklarē, ka Radiolan atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo *NETGEAR Inc.* deklaruoja, kad šis Radiolan atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Nederlands [Dutch]	Hierbij verklaart *NETGEAR Inc.* dat het toestel Radiolan in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
Malti [Maltese]	Hawnhekk, *NETGEAR Inc.*, jiddikjara li dan Radiolan jikkonforma mal-htigijiet essenzjali u ma provvedimenti ohrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Hungarian]	Alulírott, *NETGEAR Inc.* nyilatkozom, hogy a Radiolan megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Polski [Polish]	Niniejszym NETGEAR Inc. oświadcza, że Radiolan jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portuguese]	*NETGEAR Inc.* declara que este Radiolan está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	NETGEAR Inc. izjavlja, da je ta Radiolan v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	*NETGEAR Inc.* týmto vyhlasuje, že Radiolan spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	*NETGEAR Inc.* vakuuttaa täten että Radiolan tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska [Swedish]	Härmed intygar *NETGEAR Inc.* att denna Radiolan står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

Íslenska [Icelandic]	Hér með lýsir *NETGEAR Inc.* yfir því að Radiolan er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.
Norsk [Norwegian]	*NETGEAR Inc.* erklærer herved at utstyret *Radiolan* er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.

This device is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 - 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

FCC Requirements for Operation in the United States

FCC Information to User

This product does not contain any user serviceable components and is to be used with approved antennas only. Any product changes or modifications will invalidate all applicable regulatory certifications and approvals.

FCC Guidelines for Human Exposure

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 20 cm between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Declaration of Conformity

We, NETGEAR, Inc., 350 East Plumeria Drive, San Jose, CA 95134, declare under our sole responsibility that the ProSafe Wireless-N 8-Port Gigabit VPN Firewall FVS318N complies with Part 15 Subpart B of FCC CFR47 Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

FCC Radio Frequency Interference Warnings & Instructions

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following methods:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an electrical outlet on a circuit different from that which the radio receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution

- Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.
- This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

- For product available in the USA market, only channel 1~11 can be operated. Selection of other channels is not possible.
- This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (ProSafe Wireless-N 8-Port Gigabit VPN Firewall FVS318N) does not exceed the Class B limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

This Class [B] digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe [B] est conforme à la norme NMB-003 du Canada

Industry Canada

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE: Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Caution:

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

NOTE IMPORTANTE: Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

GPL License Agreement

GPL may be included in this product; to view the GPL license agreement go to *ftp://downloads.netgear.com/files/GPLnotice.pdf*.

For GNU General Public License (GPL) related information, please visit *http://support.netgear.com/app/answers/detail/a_id/2649*.

Interference Reduction Table

The following table shows the Recommended Minimum Distance between NETGEAR equipment and household appliances to reduce interference (in feet and meters).

Household Appliance	Recommended Minimum Distance (in feet and meters)
Microwave ovens	30 feet / 9 meters
Baby Monitor - Analog	20 feet / 6 meters
Baby Monitor - Digital	40 feet / 12 meters
Cordless phone - Analog	20 feet / 6 meters

Household Appliance	Recommended Minimum Distance (in feet and meters)
Cordless phone - Digital	30 feet / 9 meters
Bluetooth devices	20 feet / 6 meters
ZigBee	20 feet / 6 meters

Index

Numerics

10BASE-T, 100BASE-T, and 1000BASE-T speeds 44
2.4-GHz wireless mode 87
20- and 40-MHz channel spacing 87
3322.org 40–42
64-bit and 128-bit WEP 96
6to4 tunnels 37, 71
802.11b/bg/ng/n data rates and frequencies 335
802.11b/bg/ng/n modes 87

A

AAA (authentication, authorization, and accounting) 196
access
  remote management 278
  restricting by MAC address 101
access point
  default settings 333
  name 100
account name, PPTP and PPPoE 28
action buttons (web management interface) 22
Active LED 16
active users, IPSec VPN, SSL VPN, and L2TP 307–308
ActiveX
  blocking 143
  web cache cleaner, SSL VPN 226
AD (Active Directory)
  configuration 249
  description 246
address autoconfiguration, IPv6 33
address pools, Mode Config operation 201
address reservation 64
Address Resolution Protocol (ARP)
  broadcasting, configuring 57
  requests 59
addresses (IPv4 and IPv6), requirements and errors 23
administrator
  default name and password 20
  receiving logs by email 296
  settings (admin) 276
  user account 256
advertisement prefixes, IPv6 70
advertisement, UPnP information 154
AES (Advanced Encryption Standard)
  IKE policy settings 184
  Mode Config settings 201
  VPN policy settings 192–193
ALG (Application Level Gateway) 135
antennas
  external orientation 85
  rear panel 17
Application Level Gateway (ALG) 135
ARP (Address Resolution Protocol)
  broadcasting, configuring 57
  requests 59
arrow (web management interface) 22
attached devices
  monitoring with SNMP 281
  viewing 314
attack checks 132
authentication
  for IPSec VPN
    pre-shared key 158, 162, 185
    RSA signature 185
  for SSL VPN 249
  network 91
  See also
    AD (Active Directory)
    LDAP (Lightweight Directory Access Protocol)
    MIAS (Microsoft Internet Authentication Service)
    RADIUS authentication
    WiKID
authentication domain 247, 255
authentication, authorization, and accounting (AAA) 196
Auto Uplink, autosensing Ethernet connections 12
autodetecting IPv4 Internet settings 26
automatically configuring IPv6 Internet connection 33
autosensing port speed 44

B

b mode, wireless 87

backing up configuration file 285
bandwidth capacity 270
bandwidth limits, logging dropped packets 295
bandwidth profiles
  creating 139–141
  shifting traffic mix 276
basic service set (BSS) 91
basic service set identifier (BSSID) 91
beacon interval 104
blocking
  instant messaging applications 131
  sites to reduce traffic 272
  TCP flood 133
  traffic, action when reaching limit 293
  UDP flood 133
broadband
  advanced settings (IPv4 and IPv6) 44
  classical routing (IPv4) 31
  IPv4 connection status 26, 311
  IPv6 connection status 34, 312
  IPv6 mode, configuring 36
  NAT (IPv4), configuring 31
broadcasting wireless network names (SSIDs) 89, 95
browsers
  user login policies 260
  web management interface 19
BSS (basic service set) 91
BSSID (basic service set identifier) 91
buttons (web management interface) 22

C

CA (certification authority) 187, 262–269
cache control, SSL VPN 226
capturing packets 318
Carrier Sense Multiple Access (CSMA) 105
CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) 90, 96
certificate revocation list (CRL) 264, 269
certificate signing request (CSR) 265
certificates
  commercial CAs 263
  CRL 264, 269
  CSR 265
  overview 262
  self-signed 263–265
  signature key length 267
  trusted 263–264
certification authority (CA) 187, 262–269
channel spacing, wireless 87
channels and frequencies, selecting 88
CHAP (Challenge Handshake Authentication Protocol) 246
  See also
    MIAS (Microsoft Internet Authentication Service)
    RADIUS authentication
    WiKID
classical routing (IPv4), configuring 31
Clear to Send (CTS) packets and self-protection 105
client identifier 30
clients, wireless separation 100
collision detection and collision avoidance, CSMA 105
community strings, SNMP 282
compatibility, protocols and standards 333
compliance, notification of 344
compliance, regulatory
  wired products 340–343
concatenating IPv6 addresses 38
configuration file, managing 284–286
configuration manager (web management interface)
  login 19
  menu 22
configuration settings, defaults 331
connection reset, PPPoE broadband connection 29
connection type and state (WAN), viewing 306
connectivity, testing 45
console port 17
content filtering, configuring 143
control side band 87
cookies, blocking 143
Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) 90, 96
counter, WAN traffic 292
country, wireless radio 87
CRL (certificate revocation list) 264, 269
crossover cable 12, 321
CSMA (Carrier Sense Multiple Access) 105
CSR (certificate signing request) 265
CTS (Clear to Send) packets and self-protection 105
custom services, firewall 136

D

Data Encryption Standard. *See* DES.
data rates, 802.11b/bg/ng/n 335
database, local users 248
date and daylight saving time
  settings 289
  troubleshooting settings 330
DC power plug receptacle 17
DDNS (dynamic DNS), configuring 40–42

Dead Peer Detection (DPD) 185, 216
defaults
configuration settings 331
configuration, restoring 328
factory 286, 328
firewall IPv4 address and subnet mask 53
IPSec VPN Wizard 157
login time-out 21
MTU 44
password 20, 328
PVID 47
user name 20
demilitarized zone. *See* DMZ.
denial of service. *See* DoS.
DES (Data Encryption Standard) and 3DES 184, 192–193, 201
DH (Diffie-Hellman) groups 180, 185, 194, 201
DHCP (Dynamic Host Configuration Protocol)
automatic configuration of devices 12
DNS servers, IPv4 addresses 54, 74
domain name 54, 74
LDAP server 55, 75
lease time 54, 74
log, monitoring 315
relay 74
relay, VLANs 50, 54
server 74
server, VLANs 49, 53
DHCPv6, stateless and stateful 33, 66
diagnostics tools 316
Diffie-Hellman (DH) groups 180, 185, 194, 201
digital certificates. *See* certificates.
dimensions 334
dipole antenna 17
direction, bandwidth profiles 140
DMZ (demilitarized zone)
configuring 72–75
increasing traffic 274
port 12, 16
DNS (Domain Name Server)
automatic configuration of PCs 12
dynamic 40–42
looking up an address 317
Mode Config address allocation 201
proxy 13, 75
proxy, VLANs 50, 55
server IPv4 addresses
broadband settings 30
DMZ settings 74
LAN/VLAN settings 54
SSL VPN settings 231
server IPv6 addresses, broadband settings 35
documentation, online 330
domain name blocking 143
Domain Name Server. *See* DNS.
domain name, PPTP and PPPoE connections 28
domains for authentication 247, 255
DoS (denial of service)
attack check settings 133
default protection 11, 112
DPD (Dead Peer Detection) 185, 216
DTIM (Delivery Traffic Indication Message) interval 104
duplex, half and full 44
dynamic DNS (DDNS), configuring 40–42
Dynamic Host Configuration Protocol (DHCP)
WINS server 54, 74
Dynamic Host Configuration Protocol. *See* DHCP.
dynamically assigned IPv4 addresses 30
DynDNS.org 40–42

E

e-commerce 221
edge device, configuring XAUTH 196
electromagnetic emissions 334
emailing logs 296
encryption
WEP 96, 97
WPA, WPA2, and mixed mode 96
environmental specifications 334
ESS (extended service set) 91
Ethernet ports 14
event logs 295
exchange mode, IKE policies 180, 183
exposed hosts
increasing traffic 275
specifying 130
extended authentication (XAUTH)
configuring 194–196
IKE policies 186
extended authentication. *See* XAUTH.
extended service set (ESS) 91
extension channels 87

F

factory default settings
list of 331
reverting to 286
FE80 IPv6 addresses 64
firewall
attack checks 132
bandwidth profiles 139–141
custom services 136

default settings 332
inbound rules. *See* inbound rules.
outbound rules. *See* outbound rules.
overview 11
QoS profiles 142
rules
See also inbound rules.
See also outbound rules.
numbers and types supported 109
order of precedence 115
scheduling 146
firmware, upgrading 287
flags, router advertisements 70
FQDNs (fully qualified domain names)
DDNS requirements 41
IPSec VPN, configuring endpoints 158, 162, 184
SSL VPN, configuring port forwarding 223
fragmentation length 105
frames, jumbo 134
frequencies 802.11b/bg/ng 335
frequencies and channels, selecting 88
front panel, ports and LEDs 14
full tunnel, SSL VPN 230
fully qualified domain names. *See* FQDNs.

G

g mode, wireless 87
gateway, ISP
IPv4 address 30
IPv6 address 35
generating keys, WEP 96
global addresses, IPv6 38
group and global policies, configuring for SSL VPN 235
groups
LAN groups 61–63
VPN policies 251
guests, user account 255–256
GUI (graphical user interface)
description 21
troubleshooting 321

H

hardware
front panel ports and LEDs 15
rear panel, components 17
Help button (web management interface) 23
hosts
exposed, increasing traffic 275
exposed, specifying 130
name resolution 229
public web server 126
humidity, operating and storage 334

I

ICMP (Internet Control Message Protocol)
time-out 135
type 138
idle time-out, broadband connection 29
IGP (Interior Gateway Protocol) 78
IKE policies
exchange mode 180, 183
ISAKMP identifier 180, 184
managing 179
Mode Config operation 183, 202
XAUTH 186
inbound rules
default 108
DMZ-to-WAN rules 121
examples 126
increasing traffic 273
LAN-to-DMZ rules 125
LAN-to-WAN rules 118
order of precedence 115
overview 112
scheduling 146
settings 113–114
inbound traffic, bandwidth 140
increasing traffic
overview 273–275
port forwarding 112
infrastructure mode 89
installation, verifying 45
instant messaging applications, blocking 131
interface specifications 334
interference (wireless) 85
Interior Gateway Protocol (IGP) 78
Internet connection
configuring 19
default settings 332
Internet Control Message Protocol (ICMP)
time-out 135
type 138
Internet Key Exchange. *See* IKE policies.
Internet service provider (ISP)
connection, troubleshooting 323
gateway IPv4 address 30
gateway IPv6 address 35
Internet service provider. *See* ISP.
Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) tunnel 38
IP/MAC binding 148
IPSec hosts, XAUTH 195–196

IPSec VPN Wizard
client-to-gateway tunnels, setting up 161
default settings 157
description 13
gateway-to-gateway tunnels, setting up 156
IPSec VPN. *See* VPN tunnels.
IPv4 addresses
autogenerated 321
default 53
DHCP, address pool 74
DMZ port 73
DNS servers 30, 54, 74
dynamically assigned 30
errors 23
ISATAP tunnel address 39
LAN, secondary 57–59
MAC binding 148
port forwarding, SSL VPN 228
reserved 64
secondary LAN 57
static or permanent 26, 30
subnet mask, default 53
subnet mask, DMZ port 73
IPv4 gateway 30
IPv4 Internet connection
auto-detecting 25
manually configuring 27
setting up 24
IPv4 ISP, logging in 28
IPv4 routing modes 31
IPv6 addresses
advertisement prefixes 70
autoconfiguration 33, 66
concatenating 38
DHCPv6, stateless and stateful configuring 33, 66
DNS servers 35
errors 23
FE80 64
LAN address pools 67
LAN setup 65
link-local address 64
private address 38
route destination 82
static or permanent 35
unique global address 38
IPv6 gateway 83
IPv6 Internet connection
automatically configuring 33
manually configuring 34
setting up 24
IPv6 mode, configuring 36
IPv6 prefixes 35, 39, 82
IPv6 tunnel status, viewing 40
IPv6 tunnels 37–40, 71
ISAKMP identifier 180, 184
ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) tunnel 38
ISP (Internet service provider)
connection, troubleshooting 323
gateway IPv4 address 30
gateway IPv6 address 35

J

Java, blocking 142
jumbo frames 134

K

keep-alives, VPN tunnels 191, 215
key generation, WEP 97
keyword blocking 143
knowledge base 330

L

L2TP (Layer 2 Tunneling Protocol) server 218
L2TP Access Concentrator (LAC) 218
L2TP users 256, 262
LAC (L2TP Access Concentrator) 218
LAN
address pools (IPv6) 67
bandwidth capacity 270
default settings (IPv4) 332
groups, assigning and managing 61–63
IPv4 settings, configuring 48
IPv6 settings, configuring 64
Known PCs and Devices table 61
network database 59–62
port status, viewing 305
secondary IPv4 addresses 57
testing the LAN path 327
LAN groups, keyword blocking 145
LAN LEDs 16, 321
LAN ports 10, 14
LAN security checks 133
Layer 2 Tunneling Protocol (L2TP) server 218
LDAP (Lightweight Directory Access Protocol)
description 246
domain authentication 249
server, DHCP 55, 75
VLANs 50
lease and rebind time, DHCPv6 66
LEDs (front panel)
explanation of 15
troubleshooting 320–321
lifetime, router 70

Lightweight Directory Access Protocol. *See* LDAP.
limit, traffic meter (or counter) 292
limits, sessions 134
link-local addresses, IPv6 64
link-local advertisements, IPv6 68
local area network. *See* LAN.
local user database 248
location of wireless VPN firewall 18
lock, security 17
login attempts 295
login default settings 331
login policies, user 257–260
login time-out
  changing 261, 276
  default 21
logs, configuring 295
long preamble 105
looking up DNS address 317
losing wireless connection 102
lower side band 87

M

MAC addresses
  blocked, adding 147
  configuring 31, 36, 44
  format 44, 148
  IP binding 148
  restricting wireless access by 89, 101
  spoofing 324
  VLANs, unique 56
main navigation menu (web management interface) 22
managed RA flag 70
management default settings 332
maximum transmission unit (MTU)
  default 44
  IPv6 packets 70
MD5
  IKE polices 184
  Mode Config setting 202
  RIP-2 80
  self-signed certificate requests 267
  VPN policies 193
Media Access Control. *See* MAC addresses.
Message-Digest algorithm 5. *See* MD5.
metering WAN traffic 290
metric
  static IPv4 routes 77
  static IPv6 routes 83
MIAS (Microsoft Internet Authentication Service)
  description 246
  MIAS-CHAP and MIAS-PAP 249
Mode Config operation
  configuring 199–206
  record 183
mode, wireless 87
MTU (maximum transmission unit)
  default 44
  IPv6 packets 70
multicast pass-through 134
multihome LAN IPv4 addresses, configuring 57–59

N

n and ng modes, wireless 87
names, changing
  DDNS host and domain 42
  ISP login 28
  known PCs and devices 61
  LAN groups 63
  PPTP and PPPoE accounts 28
  wireless access points 100
  wireless profiles and SSIDs 94
NAS (Network Access Server) 198
NAT (Network Address Translation)
  configuring 31
  description 12
  firewall, use with 107
  mapping, one-to-one 31, 128
  status, viewing 306
NDP (Neighbor Discovery Protocol) 68
NetBIOS, VPN tunnels 191, 218
Network Access Server (NAS) 198
Network Address Translation. *See* NAT.
networks
  authentication 91
  database 59–62, 314
  diagnostic tools 316
  resources, SSL VPN 233
newsgroup 143
NT domain 246, 249
NTP (Network Time Protocol)
  servers, settings 289
  troubleshooting 330

O

On/Off switch 17
one-time passcode (OTP) 336–338
online documentation 330
online games, DMZ port 72
open system (no wireless security) 95
operating frequency, radio 87
option arrow (web management interface) 22
Oray.net 40–42

order of precedence, firewall rules 115
OTP (one-time passcode) 336–338
outbound rules
default 108
DMZ-to-WAN rules 121
examples 131
LAN-to-DMZ rules 124
LAN-to-WAN rules 117
order of precedence 115
overview 109
QoS profile 111
reducing traffic 271
scheduling 146
service blocking 109
settings 110–111
outbound traffic, bandwidth 140

P

package contents, wireless VPN firewall 14
packets
accepted and dropped 295
capturing 318
transmitted, received, and collided 303
PAP (Password Authentication Protocol) 246
See also
MIAS (Microsoft Internet Authentication Service)
RADIUS authentication
WiKID
partition, WLAN 100
passphrase, WEP, WPA, WPA2, and mixed mode 96
pass-through, multicast 134
passwords
changing 261, 276
default 20
restoring 328
Perfect Forward Secrecy (PFS) 194, 201
performance management 270
permanent addresses
IPv4 address 26, 30
IPv6 address 35
PFS (Perfect Forward Secrecy) 194, 201
PIN method, WPS 103
pinging
checking connections 316
responding on Internet ports 132
responding on LAN ports 133
troubleshooting TCP/IP 327
using the ping utility 316
placement of wireless VPN firewall 18, 85
plug and play (UPnP), configuring 153
Point-to-Point Tunneling Protocol (PPTP) settings 26, 28
policies
IKE
exchange mode 180, 183
ISAKMP identifier 180, 184
managing 179
Mode Config operation 183, 202
XAUTH 186
IPSec VPN
automatically generated 187
groups, configuring 251
managing 179
manually generated 187
SSL VPN
managing 235
settings 238
policy hierarchy 235
pools, Mode Config operation 201
port filtering
reducing traffic 271
rules 109
port forwarding
firewall rules 109, 112
increasing traffic 112
reducing traffic 273
port membership, VLANs 53
port numbers
customized services 136
port triggering 151
SSL VPN port forwarding 228
port ranges
port triggering 152
SSL VPN policies 239–240
SSL VPN resources 235
port speed 44
port triggering
configuring 151–153
increasing traffic 274
status monitoring 153, 310
Port VLAN Identifier (PVID) 47
portals, accessing SSL VPN 241
portals, options for SSL VPN 222
ports
console 17
LAN and WAN and their LEDs 14
Power LED 15, 320
power plug receptacle and Power On/Off switch 17
power specifications 333
PPP connection 222
PPPoE (PPP over Ethernet)
description 13
settings 26, 29
PPTP (Point-to-Point Tunneling Protocol) settings 26, 28

preamble type 105
preference, router (IPv6) 70
prefixes, IPv6 35, 39, 82
pre-shared key
  client-to-gateway VPN tunnel 162
  gateway-to-gateway VPN tunnel 158
  IKE policy settings 185
  WPA, WPA2, and mixed mode 96
private addresses, IPv6 38
profiles
  bandwidth 139–141
  QoS 141
  VLANs 48–55
  wireless security 91, 93–97
protection from common attacks 132
protocols
  compatibilities 333
  RIP 12
  service numbers 137
  traffic volume by protocol 293
PSK. *See* pre-shared key.
public web server, hosting 126
Push 'N' Connect 102
Push button configuration (PBC) method, WPS 103
PVID (Port VLAN Identifier) 47

Q

QoS (Quality of Service)
  profiles 141
  shifting traffic mix 275
question mark icon (web management interface) 23

R

radio, configuring
  advanced settings 104
  basic settings 86
RADIUS authentication
  CHAP and PAP
    domain authentication 249
    XAUTH 186, 195–196
  description 246
  MSCHAP(v2), domain authentication 249
RADIUS server, configuring 197–198
RADVD (Router Advertisement Deamon) 68
range guidelines, wireless equipment 85
RAs (router advertisements) 69
read-only and read-write access 255
rebooting 318
reducing traffic 270–272
region, wireless radio 87
regulatory compliance
  wired products 340–343
relay gateway 54, 74
Remote Authentication Dial In User Service
  See RADIUS authentication.
  See RADIUS server.
remote management access 278
remote users, assigning addresses (Mode Config) 198
Request to Send (RTS) threshold 105
reserved IPv4 addresses, configuring 64
restoring, configuration file 286
restricting wireless access by MAC address 89
RFC 1349 141
RFC 1700 137
RFC 2865 196
RIP (Routing Information Protocol), configuring 78–80
roaming 91
Router Advertisement Deamon (RADVD) 68
router advertisements (RAs) and router lifetime (IPv6) 69
Routing Information Protocol (RIP), configuring 78–80
routing logs 295
routing modes
  IPv4 31
  IPv6 (IPv4-only and IPv4/IPv6) 36
routing table
  adding static IPv4 routes 76
  adding static IPv6 routes 81
  displaying 317
RSA signatures 185
RTS (Request to Send) threshold 105
rules
  See inbound rules.
  See outbound rules.

S

SA (security association)
  IKE policies 180, 184
  IPSec VPN Wizard 156
  Mode Config operation 201
  VPN connection status 178
  VPN policies 192, 193
scheduling firewall rules 146
secondary LAN IPv4 addresses, configuring 57–59
Secure Hash Algorithm 1. *See* SHA-1.
security association. *See* SA.
security checks, LAN 133
security lock receptacle 17
Security Parameters Index (SPI) 192
security profiles, wireless
  creating and configuring 93–97

description 89–92
separation, wireless 100
server preference, DHCPv6 66
service blocking
reducing traffic 271
rules, firewall 109
service numbers, common protocols 137
Session Initiation Protocol (SIP) 135
session limits
configuring 134
logging dropped packets 295
severities, syslog 297
SHA-1
IKE policies 184
Mode Config operation 202
self certificate requests 267
VPN policies 193
shared key, WEP 96
short preamble 105
shutting down 318
side band, control 87
signature key length 267
Simple Network Management Protocol (SNMP)
configuring 281–284
description 13
SIP (Session Initiation Protocol) 135
sit0-WAN1 (6to4 tunnel) 37
SLA ID (Site Level Aggregation Identifier) 70
sniffer 322
SNMP (Simple Network Management Protocol)
configuring 281–284
description 13
software, upgrading 287
source MAC filtering
configuring MAC addresses 147
logging matched packets 295
reducing traffic 272
spacing, channels 87
specifications, physical and technical 333
speed, ports 44
SPI (Security Parameters Index) 192
SPI (Stateful Packet Inspection) 11, 108
split tunnel, SSL VPN 230
spoofing MAC addresses 324
SSIDs (service set identifiers)
assigning a name and broadcasting 94
broadcasting and security 89
SSL VPN
ActiveX web cache cleaner 226
ActiveX-based client 222
authentication 249
cache control 226
client IP address range and routes 230–232
configuration steps 222
connection status 243
FQDNs, configuring port forwarding 223
logs 244
network resources 233
overview 11
policies
managing 235
settings 238
port forwarding
configuring 227–229
description 222
portal
accessing 241
options 222
settings, configuring 223
specifications 335
tunnel description 222
user account 255–256
user portal 242
Stateful Packet Inspection 11, 108
stateless and stateful IPv6 addresses, autoconfiguration 33, 66
static addresses
IPv4 address 26, 30
IPv6 address 35
static routes
IPv4 routes
configuring 76–81
routing table 76
IPv6 routes
configuring 81–83
routing table 81
statistics, viewing 302
status screens 300–315
stealth mode 133
submenu tabs (web management interface) 22
SYN flood 133
syslog server 297
system
date and time settings, configuring 288
logs 295
status, viewing 300–307
updating firmware 287

T

table buttons (web management interface) 22
tabs, submenu (web management interface) 22
TCP (Transmission Control Protocol) 152
TCP flood, blocking 133

TCP time-out 135
TCP/IP network, troubleshooting 327
technical specifications 333
technical support 2, 318
temperatures, operating and storage 334
Temporal Key Integrity Protocol (TKIP) 90, 96
Test LED 15, 320
testing connectivity 45
testing wireless connectivity 105
time settings
  configuring 289
  troubleshooting 330
time-out
  error, troubleshooting 322
  sessions 135
timer, virtual access points 100
tips, firewall and content filtering 108
TKIP (Temporal Key Integrity Protocol) 90, 96
ToS (Type of Service), QoS profile 111
tracert, using with DDNS 281
tracing a route (traceroute) 317
trademarks 2
traffic
  action when reaching limit 293
  bandwidth 139–141
  diagnostic tools 316
  increasing 273–275
  managing 270
  reducing 270–272
  volume by protocol 293
traffic meter (or counter) 290
Transmission Control Protocol (TCP) 152
transmit power and rate, radio 88
troubleshooting
  basic functioning 320
  browsers 322
  configuration settings, using sniffer 322
  date and time settings 330
  defaults 322
  IP addresses, requirements 23
  ISP connection 323
  LEDs 320–321
  NTP 330
  testing your setup 328
  time-out error 322
  web management interface 321
trusted certificates 263–264
trusted domains, building a list of 145
tunnels, IPv6 37–40, 71
two-factor authentication
  authentication, overview 336
  description 246
  WiKID-PAP and WiKID-CHAP 249
Type of Service (ToS), QoS profile 111
TZO.com 40–42

U

UDP (User Datagram Protocol) 152
UDP flood, blocking 133
UDP time-out 135
unicast packets, IPv6 69
Universal Plug and Play (UPnP), configuring 153
unsolicited multicast packets, IPv6 69
upgrading firmware 287
UPnP (Universal Plug and Play), configuring 153
upper side band 87
user accounts, configuring 254
User Datagram Protocol (UDP) 152
user name, default 20
user passwords, changing 261
user policies, configuring for SSL VPN 235
user portal 242
user types 255–257, 262
users
  active VPN and L2TP 307–308
  administrative (admin) settings 276
  assigned groups 256
  login policies, configuring 257–260
  login time-out 261

V

VAPs (virtual access points), configuring 98
vendor class identifier (VCI) 30
videoconferencing
  DMZ port 72
  from restricted address 127
virtual access points (VAPs), configuring 98
virtual LAN. *See* VLAN.
Virtual Private Network Consortium (VPNC) 13, 156
VLANs
  advantages 47
  description 46
  DHCP options 49–50
  identifiers (IDs) 91
  MAC addresses 56
  port-based 47
  profiles, configuring 51–56
VoIP (voice over IP) sessions 135
VPN client
  Configuration Wizard, using 164
  configuring manually 168
  Mode Config tunnel, opening 213

Mode Config, configuring 206
tunnel, opening 175
VPN IPSec Wizard. *See* IPSec VPN Wizard.
VPN tunnels
active users 307–308
client policy, creating 164
client-to-gateway, using IPSec VPN Wizard 161
connection status 177
DPD (Dead Peer Detection) 216
FQDNs, configuring endpoints 158, 162, 184
gateway-to-gateway, using IPSec VPN Wizard 156
IKE policies
exchange mode 180, 183
ISAKMP identifier 180, 184
managing 179
Mode Config operation 183, 202
XAUTH 186
increasing traffic 275
IPSec VPN
logs 178
specifications 334
IPSec VPN policies
automatically generated 187
groups, configuring 251
managing 179
manually generated 187
IPSec VPN user account 255–256
keep-alives 191, 215
NetBIOS 191, 218
pass-through (IPSec, PPTP, L2TP) 133
pre-shared key
client-to-gateway tunnel 162
gateway-to-gateway tunnel 158
IKE policy settings 185
RSA signature 185
sending syslogs 297
testing connections 175
XAUTH 194–196
VPNC (Virtual Private Network Consortium) 13, 156

W

WAN
bandwidth capacity 270
connection type and state, viewing 306
WAN LEDs 16, 321
WAN ports 14
WAN traffic meter (or counter) 290
web component blocking 142
web management interface
description 21
troubleshooting 321
weight 334
WEP (wired equivalent privacy)
configuring 95–96
types of encryption 89
Wi-Fi Multimedia (WMM) 105
Wi-Fi protected access (WPA), WPA2, and mixed mode
configuring 95–97
types of encryption 89
Wi-Fi Protected Setup (WPS) 102
WiKID
authentication, overview 336
description 246
WiKID-PAP and WiKID-CHAP 249
WINS server
DHCP 54, 74
Mode Config operation 201
wired equivalent privacy (WEP)
configuring 95–96
types of encryption 89
wireless clients, separating 100
wireless connection, losing 102
wireless connectivity, testing 105
wireless equipment, placement and range 85
wireless mode 87
wireless network name (SSID)
broadcasting 94
broadcasting and security 89
wireless radio
advanced settings, configuring 104
basic settings, configuring 86
wireless security 89–98
wireless separation 100
wireless specifications 335
wireless status, viewing 307
WLAN partition 100
WMM (Wi-Fi Multimedia) 105
WPA (Wi-Fi protected access), WPA2, and mixed mode
configuring 95–97
types of encryption 89
WPS (Wi-Fi Protected Setup) 102

X

XAUTH (extended authentication)
configuring 194–196
IKE policies 186